

ipTIME 웹 설정 설명서

문의 사항 및 고객 지원

Tel. 070-7018-1199
<http://www.iptime.co.kr>

(주) 이에프엠네트웍스

사용자 설명서 보는 방법

- 1장 ~ 5장의 내용에 따라 PC를 설정하고 ipTIME의 인터넷 연결을 설정하면 공유기에 연결된 PC에서 인터넷을 사용할 수 있습니다.
- 설명서 1~3장은 공유기와 PC를 연결하는 방법, 공유기에 인터넷을 연결하는 방법이 기술되어 있습니다.
- 설명서 4장은 유선으로 연결된 PC에서 공유기에 내장된 AP를 설정하는 방법, 무선 랜이 장착된 PC를 공유기에 연결하는 방법이 기술되어 있습니다.
- 6장 ~ 12장은 ipTIME의 모든 기능을 설명하는 설명서입니다. 제품 사용시 필요한 기능에 해당하는 부분의 사용법을 참고하시기 바랍니다.

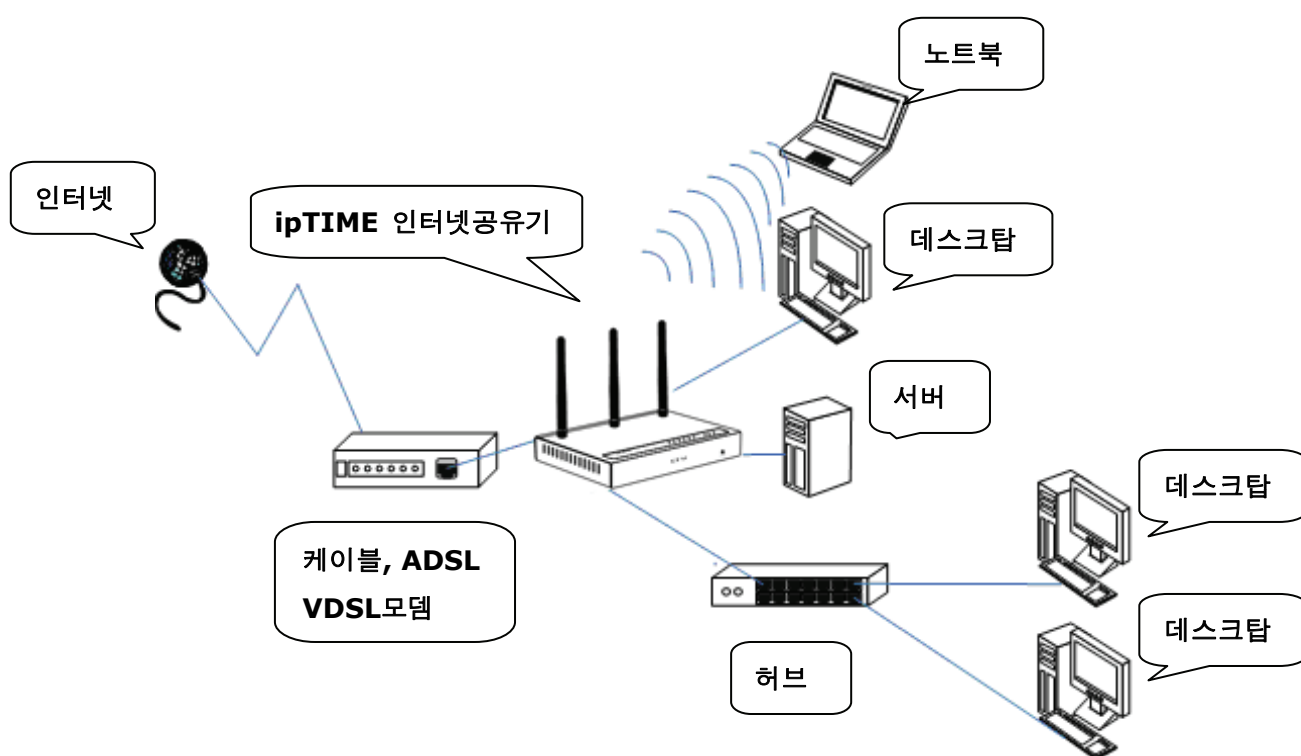
목차

1장 PC 환경 설정	7
1.1 윈도우 98/ME 설정	7
1.2 윈도우 2000 설정	11
1.3 윈도우 XP 설정	14
1.4 윈도우 VISTA 설정	17
2장 웹 설정 화면 이용하기	23
2.1 ipTIME 웹 서버 접속	23
2.2 도움말 기능	24
2.3 설정 저장 기능	25
3장 설정 마법사로 인터넷 연결	26
3.1 ipTIME 웹 서버 접속	27
3.2 ipTIME 설정 마법사 실행	28
3.3 자동 검색에 의한 PPPoE 연결 예	29
3.4 자동 검색에 의한 동적 IP 연결 예	32
3.5 수동 설정을 이용한 인터넷 연결 설정	35
4장 무선랜 연결 및 설정	41
4.1 무선 네트워크 구성	42
4.2 무선 단말 연결 방법	53
5장 기본설정	67
5.1 시스템 요약 정보	67
5.2 인터넷 연결 설정	68
5.3 무선 설정/보안	71
5.4 펌웨어 업그레이드	76

6장 네트워크 관리	78
6.1 인터넷 연결 정보	78
6.2 내부 네트워크 정보	78
6.3 인터넷 연결 설정	79
6.4 내부 네트워크 설정	79
7장 무선랜 관리	82
7.1 무선 접속 정보	82
7.2 무선 설정/보안	83
7.3 MAC 주소 인증	83
7.4 WDS 설정	84
7.5 무선 고급 설정	85
8장 NAT/라우터 관리	86
8.1 포트포워드 설정	86
8.2 포트트리거 설정	87
8.3 DMZ/Twin IP 설정	88
8.4 기타기능 설정	90
8.5 라우팅 테이블 관리	91
9장 보안기능	92
9.1 인터넷 사용제한	92
9.2 공유기 접속 관리	95
9.3 네트워크 감시	96
9.4 기타 보안 설정	99
10장 특수기능	101
10.1 카이(KAI)배틀넷	101
10.2 VPN 서버설정	103
10.3 DDNS 설정	121
10.4 WOL 기능	122

10.5 호스트검색	123
11장 트래픽관리	125
11.1 컨넥션 정보	125
11.2 링크설정/정보	126
11.3 QoS 설정	127
11.4 스위치설정	129
12장 시스템관리	130
12.1 시스템 로그	130
12.2 관리자 설정	131
12.3 펌웨어 업그레이드	131
12.4 시스템 시간 설정	132
12.5 설정 백업/복구	132
12.6 기타 설정	133
부록 A. LAN Cable 규격	134
부록 B. IP 공유기 Ping 시험	135

ipTIME 네트워크 연결 구성도



1장 PC 환경 설정

ipTIME과 연결된 모든 PC에서 **ipTIME 설치 도우미**를 따라 진행 하시면 PC의 네트워크 환경이 정상적으로 설정 됩니다.

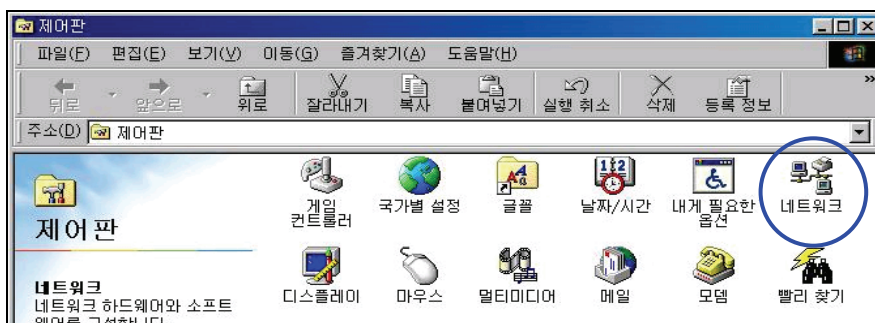
자세한 사용법은 별도로 첨부된 ipTIME 설치 도우미 설명서를 확인하시기 바랍니다.

단, Windows 98/ME 사용자는 아래의 내용을 보시고 수동으로 설정하셔야 합니다

1.1 윈도우 98/ME 설정

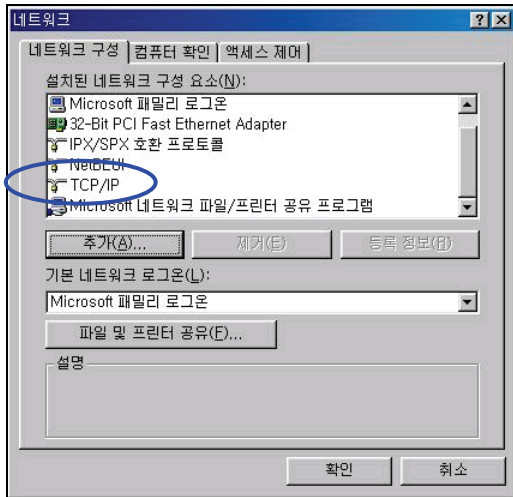
이 과정은 윈도우 98/ME의 TCP/IP 설정을 초기값으로 복원하는 것입니다. PC에 윈도우가 처음 설치된 상태라면 변경은 없으며 다음에 따라 모든 값이 정상적인지를 확인합니다.

- 윈도우 시작 버튼을 클릭한 후 메뉴에서 설정 >> 제어판을 선택합니다.
- 제어판 윈도우에서 **네트워크** 아이콘을 더블 클릭합니다.



<네트워크 아이콘 선택>

- 네트워크 구성 요소 중 TCP/IP를 더블 클릭하여 자동으로 IP 주소지정을 선택합니다.
- 전화 접속 어댑터에 연결된 TCP/IP 는 무시하고 랜 카드 관련 TCP/IP만 설정합니다.

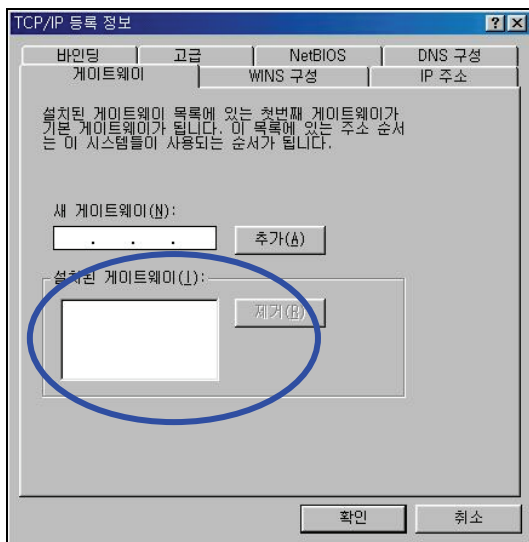


<TCP/IP 선택>

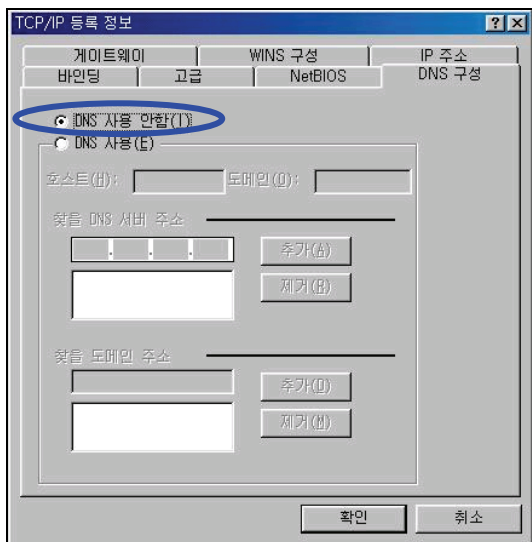


<자동 IP 주소 선택>

- 게이트웨이 항목에서 설치된 모든 게이트웨이를 제거합니다.
- DNS 구성에서 “DNS 사용 안함” 을 선택합니다.



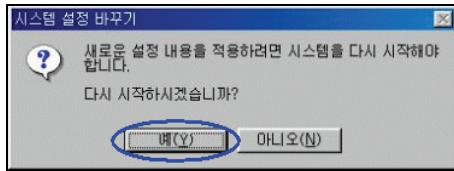
<게이트웨이 항목 전부 제거>



<DNS 사용 안함 선택>

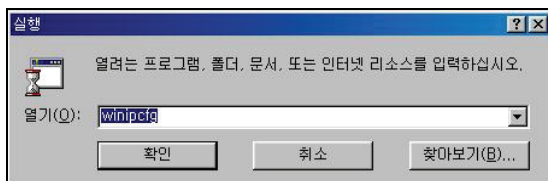
- IP주소, 게이트웨이, DNS 구성의 3가지 항목에 대한 설정이 완료되면 확인 버튼을 클릭하여 TCP/IP 등록 정보 창을 닫고 난 후, “네트워크” 창이 표시되면 다시 확인을 클릭합니다.

- 윈도우98의 경우 네트워크와 관련된 설정이 변경되면 자동으로 시스템이 재시작 됩니다. 시스템 설정 바꾸기 화면이 표시되면 “예” 를 선택하여 윈도우를 다시 시작합니다.



<시스템 재시작 확인>

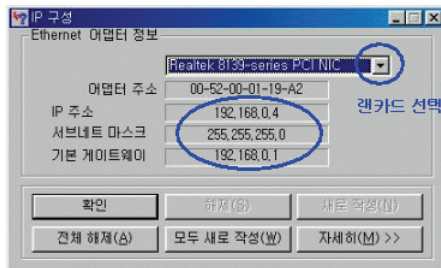
- PC가 재시작되면 ipTIME에서 IP 주소를 자동으로 할당합니다. 자동할당을 위해서 PC와 ipTIME이 LAN 케이블로 연결되어야 합니다. 만일 케이블을 연결하지 않았다면 케이블을 연결한 후 PC를 다시 시작하여야 합니다.
- IP 주소 자동 할당 확인은 winipcfg 프로그램을 이용하여 확인할 수 있습니다.
- 윈도우 [시작] 버튼을 클릭한 후 메뉴에서 실행을 선택하여 열기 항목에 그림과 같이 “winipcfg” 를 입력하고 확인 버튼을 클릭합니다.



<winipcfg 실행>

- winipcfg의 IP 구성창에서 공유기와 연결하여 사용하는 랜카드 어댑터 (NDIS 5.0 또는 해당 랜카드 선택, PPP 어댑터는 선택하면 안됨)를 선택하여 PC의 IP 주소가 192.168.0.2 ~ 192.168.0.254 사이의 값으로 자동 할당되었는지를 확인합니다. 만일 랜카드 선택에서 PPP 어댑터 이외에 사용하는 랜카드가 보이지 않을 경우에는 랜카드 드라이버를 재설치하여야 합니다. (랜카드 선택 후 “해제” 버튼을 클릭 후 “모두 새로 작성” 또는 “모두 갱신” 버튼을 클릭하여 IP할당 확인)

[참고] ipTIME 에 연결된 모든 PC는 각각 다른 IP 주소를 할당 받게 됩니다.



랜카드 선택 : NDIS 5.0 또는 해당 랜카드 선택
 어댑터 주소 : 어댑터마다 다른 값, 무시 가능
 IP 주소 : 192.168.0.2 ~ 192.168.0.254
 서브네트 마스크 : 255.255.255.0
 기본 게이트웨이 : 192.168.0.1

<IP 주소 확인>

[참고] PC의 IP 주소가 정상적으로 자동 할당되지 않는다면 다음 사항을 확인한 뒤 PC를 재시작하여 IP주소가 할당되는지 확인합니다.

- PC와 ipTIME 사이의 LAN 케이블 연결
- TCP/IP의 설정 내용 확인
- ADSL 접속 프로그램의 제거 여부

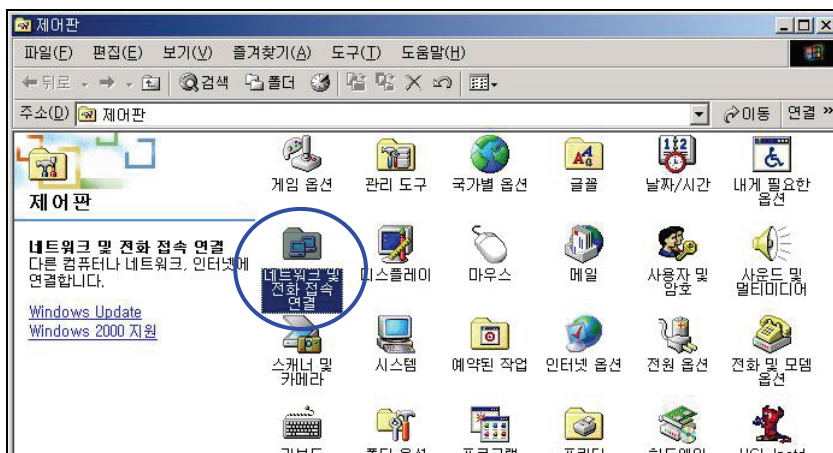
위의 사항을 확인하여도 IP 주소가 정상적으로 자동 할당되지 않는다면 당사 홈페이지 (<http://www.iptime.co.kr>)를 참고하여 IP 주소 수동 설정 방법으로 IP 주소를 설정하거나 ipTIME 고객센터(070-7018-1199)로 문의하시기 바랍니다.

PC 설정을 완료한 뒤 인터넷을 사용하기 위해서는 3장의 내용을 참고하여 설정합니다. 인터넷 연결 설정은 ipTIME에서 이루어지는 것이므로 모든 PC에서 설정할 필요는 없으며 한번만 설정하면 됩니다.

1.2 윈도우 2000 설정

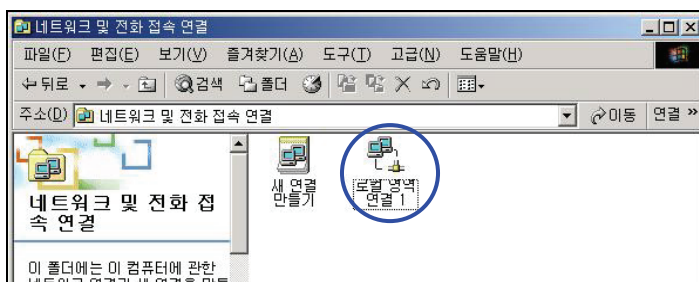
이 과정은 윈도우 2000의 TCP/IP 설정을 초기값으로 복원하는 것입니다. PC에 윈도우가 처음 설치된 상태가 아니거나 인터넷이 정상적으로 동작하지 않는다면 다음 과정에 따라 모든 값이 정상인지를 확인합니다.

- 윈도우 **시작** 버튼을 클릭한 후 메뉴에서 **설정 >> 제어판**을 선택한 뒤 **네트워크 및 전화 접속 연결** 아이콘을 더블 클릭합니다.



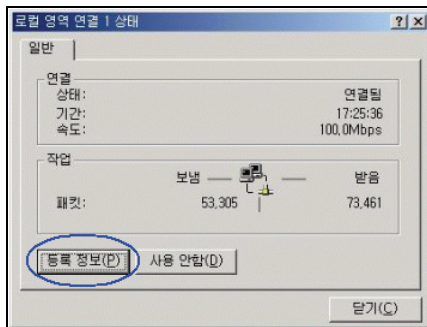
<네트워크 및 전화 접속 연결 더블 클릭>

- 네트워크 및 전화 접속 연결 윈도우에서 **로컬 영역 연결** 아이콘을 더블 클릭합니다.

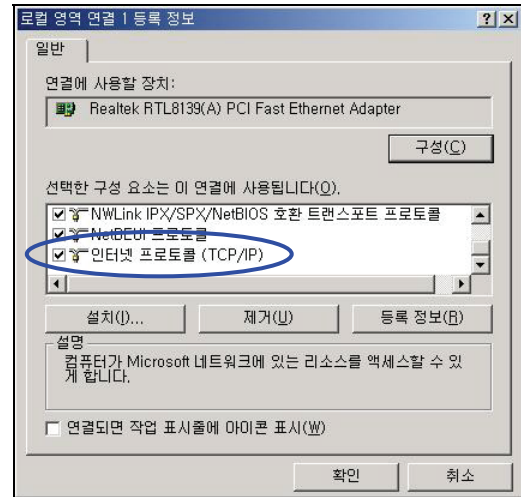


<로컬 영역 연결 더블 클릭>

- 로컬 영역 연결 윈도우에서 등록 정보를 클릭합니다.
- 등록 정보 윈도우에서 **인터넷 프로토콜 (TCP/IP)** 인터넷 프로토콜 (TCP/IP)을 더블 클릭합니다.

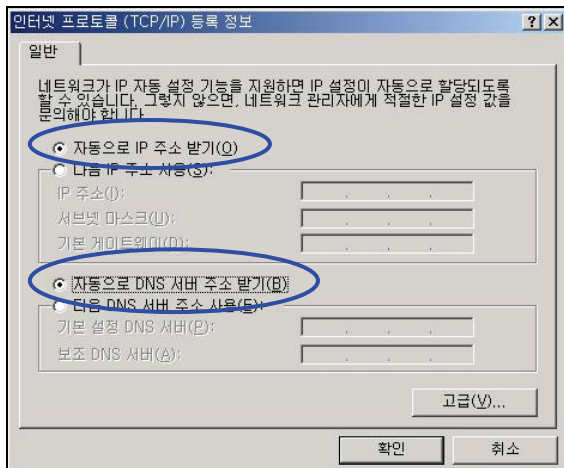


<등록 정보 선택>



<TCP/IP 더블 클릭>

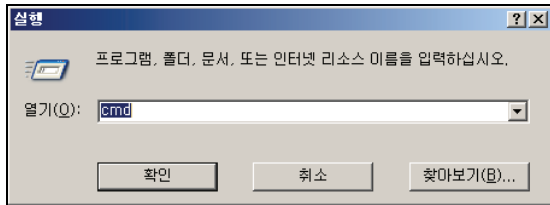
- “자동으로 IP 주소 받기”와 “자동으로 DNS 서버 주소 받기”를 선택합니다.



<자동 선택 후 확인 클릭>

- 설정완료 후 확인버튼을 클릭하고 네트워크 및 전화접속연결 창도 모두 닫습니다.
- TCP/IP 설정을 완료하면 ipTIME에서 IP 주소를 자동으로 할당합니다. 자동할당을 위해서 PC와 ipTIME이 LAN 케이블로 연결되어야 합니다. 만일 케이블을 연결하지 않았다면 케이블을 연결한 뒤 PC를 다시 시작합니다.

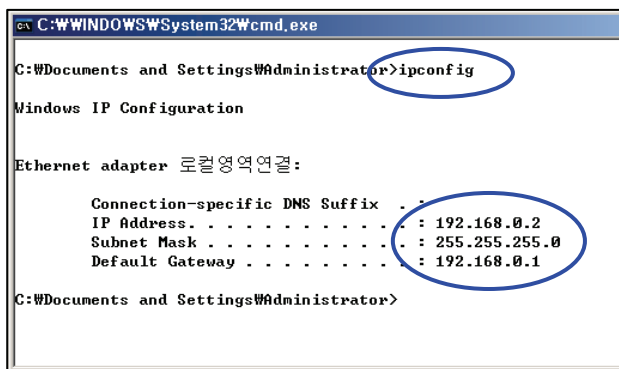
- IP 주소 자동 할당 확인은 명령 프롬프트의 **ipconfig** 명령으로 확인할 수 있습니다.
- 명령 프롬프트는 윈도우 화면 좌측 하단의 시작 버튼을 클릭한 뒤 실행을 선택하여 열기에 그림과 같이 “cmd” 를 입력하고 확인 버튼을 클릭하면 실행됩니다.



<cmd 실행>

- 명령 프롬프트가 실행되면 아래 그림과 같이 “ipconfig” 명령을 입력하여 PC에 자동 할당된 IP 주소, 서브넷 마스크, 게이트웨이 등을 확인합니다.

[참고] ipTIME에 연결된 모든 PC는 각각 다른 IP 주소를 할당 받게 됩니다.



IP Address : 192.168.0.2~254
Subnet Mask : 255.255.255.0
Default Gateway : 192.168.0.1

<IP 주소 확인>

[참고] PC의 IP 주소가 정상적으로 자동 할당되지 않는다면 다음 사항을 확인한 뒤 PC를 재시작하여 IP주소가 할당되는지 확인합니다.

- PC와 ipTIME 사이의 LAN 케이블 연결
- TCP/IP의 설정 내용 확인
- ADSL 접속 프로그램의 제거 여부

위의 사항을 확인하여도 IP 주소가 정상적으로 자동 할당되지 않는다면 당사 홈페이지 (<http://www.iptime.co.kr>)를 참고하여 IP 주소 수동 설정 방법으로 IP 주소를 설정하거나 ipTIME 고객센터(070-7018-1199)에 문의하시기 바랍니다.

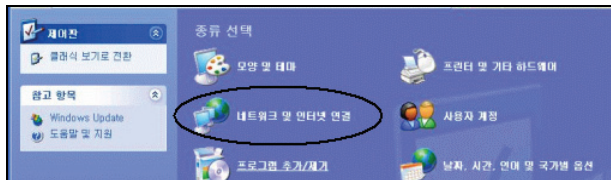
PC 설정을 완료한 뒤 인터넷을 사용하기 위해서는 3장의 내용을 참고하여 ipTIME의 WAN 포트를 인터넷에 연결 설정합니다. 인터넷 연결 설정은 공유기에서 이루어지는 것이므로 모든 PC에서 설정할 필요는 없으며 한번만 설정하면 됩니다.

1.3 윈도우 XP 설정

이 과정은 윈도우 XP의 TCP/IP 설정을 초기값으로 복원하는 것입니다. PC에 윈도우가 처음 설치된 상태라면 변경은 없으며 다음 과정에 따라 모든 값이 정상적인지를 확인합니다.

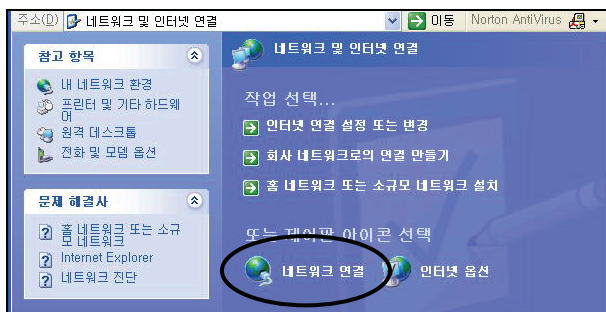
PC의 TCP/IP 설정이 완료된 후 ipTIME에서 자동으로 IP 주소를 부여 받는지 확인하기 위해서는 윈도우를 설정하기 전에 PC와 ipTIME을 LAN 케이블로 연결하고 ipTIME을 켜두어야 합니다.

- 윈도우 **시작** 버튼을 클릭한 후 메뉴에서 설정 >> 제어판을 선택합니다.
- 제어판의 **네트워크 및 인터넷 연결** 아이콘을 클릭합니다.



<네트워크 및 인터넷 연결 클릭>

- 네트워크 및 인터넷 연결에서 **네트워크 연결** 아이콘을 클릭합니다.



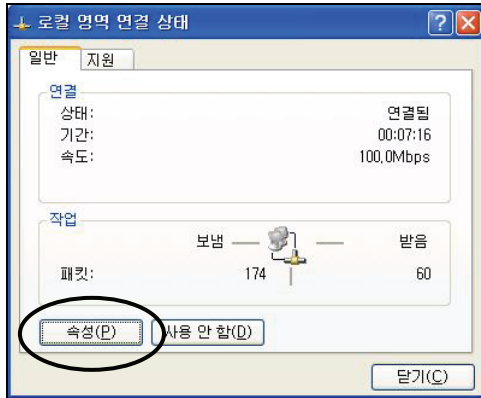
<네트워크 연결 클릭>

- 네트워크 연결에서 **로컬 영역 연결** 을 클릭하여 선택합니다.



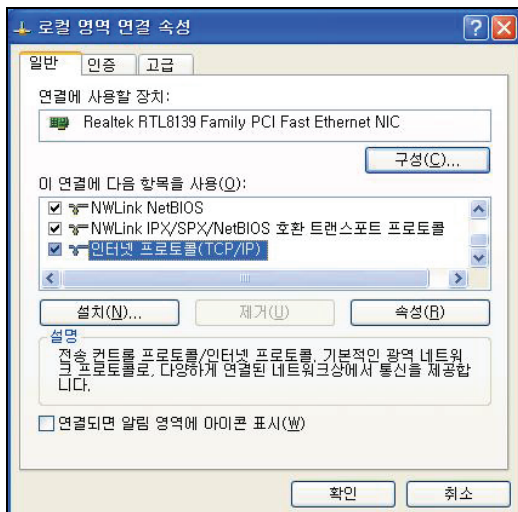
<로컬 영역 연결 클릭>

- 로컬 영역 연결 상태에서 **속성**을 클릭하여 선택합니다.

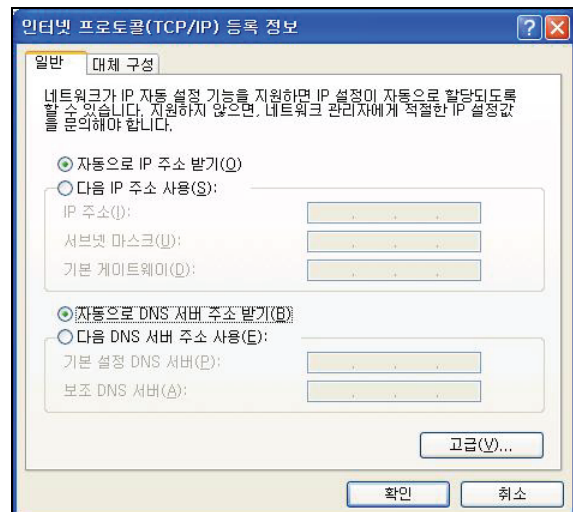


<속성 클릭>

- 인터넷 프로토콜 (TCP/IP)를 더블 클릭하여 선택하고 자동으로 IP 주소 받기와 자동으로 DNS 서버 주소 받기를 선택합니다.



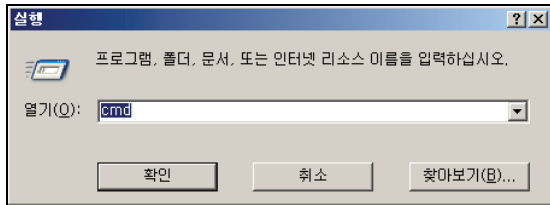
<TCP/IP 더블 클릭>



<자동 선택 후 확인 클릭>

- 설정이 완료된 뒤 확인 버튼을 클릭하고 로컬 영역 연결 속성 창도 모두 닫아 줍니다.
- TCP/IP 설정을 완료하면 ipTIME에서 IP 주소를 자동으로 할당합니다. 자동할당을 위해서 PC와 ipTIME이 LAN 케이블로 연결되어야 합니다. 만일 케이블을 연결하지 않았다면 케이블을 연결한 뒤 PC를 다시 시작합니다.

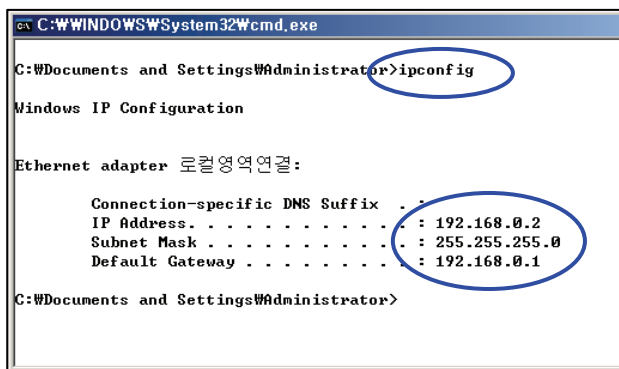
- IP 주소 자동 할당 확인은 명령 프롬프트의 **ipconfig** 명령으로 확인할 수 있습니다.
- 명령 프롬프트는 윈도우 화면 좌측 하단의 시작 버튼을 클릭한 뒤 실행을 선택하여 열기에 그림과 같이 “cmd” 를 입력하고 확인 버튼을 클릭하면 실행됩니다.



<cmd 실행>

- 명령 프롬프트가 실행되면 아래 그림과 같이 “ipconfig” 명령을 입력하여 PC에 자동 할당된 IP 주소, 서브네트마스크, 게이트웨이 등을 확인합니다.

[참고] ipTIME에 연결된 모든 PC는 각각 다른 IP 주소를 할당 받게 됩니다.



IP Address : 192.168.0.2~254
Subnet Mask : 255.255.255.0
Default Gateway : 192.168.0.1

<IP 주소 확인>

[참고] PC의 IP 주소가 정상적으로 자동 할당되지 않는다면 다음 사항을 확인한 뒤 PC를 재시작하여 IP주소가 할당되는지 확인합니다.

- PC와 ipTIME사이의 LAN 케이블 연결
- TCP/IP의 설정 내용 확인
- ADSL 접속 프로그램(광대역 연결 아이콘)의 제거 여부

위의 사항을 확인하여도 IP 주소가 정상적으로 자동 할당되지 않는다면 당사 홈페이지 (<http://www.iptime.co.kr>)를 참고하여 IP 주소 수동 설정 방법으로 IP 주소를 설정하거나 ipTIME 고객센터(070-7018-1199)에 문의하시기 바랍니다.

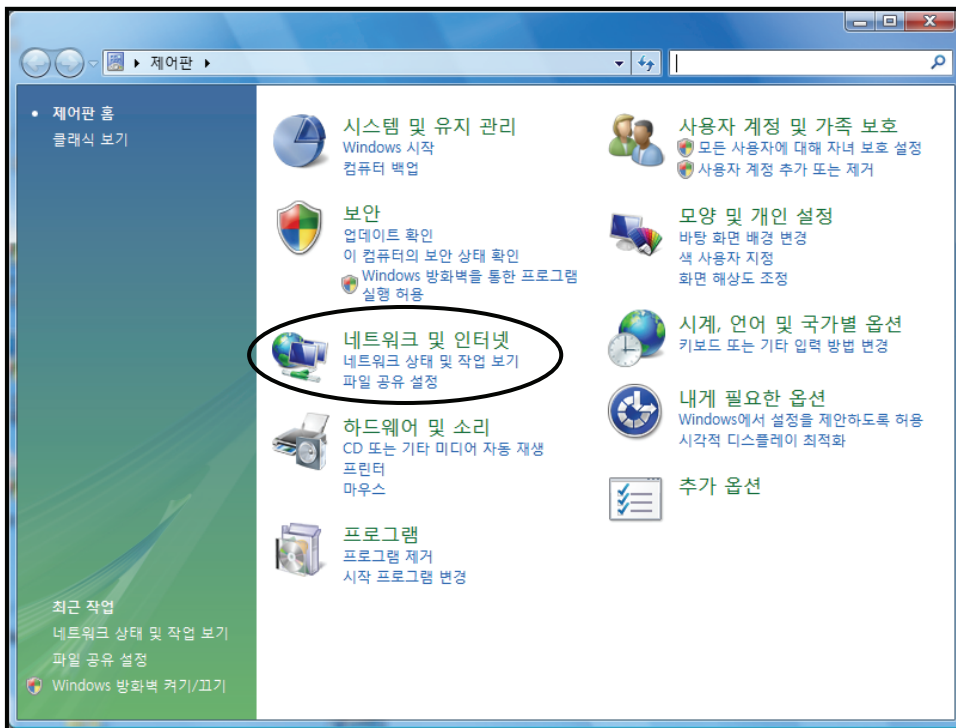
PC 설정을 완료한 뒤 인터넷을 사용하기 위해서는 3장의 내용을 참고하여 ipTIME의 WAN 포트를 인터넷에 연결 설정합니다. 인터넷 연결 설정은 공유기에서 이루어지는 것이므로 모든 PC에서 설정할 필요는 없이 한번만 설정하며, 설정 후 설정 저장을 해주시기 바랍니다

1.4 윈도우 VISTA 설정

이 과정은 윈도우 VISTA의 TCP/IP 설정을 초기값으로 복원하는 것입니다. PC에 윈도우가 처음 설치된 상태라면 변경은 없으며 다음 과정에 따라 모든 값이 정상적인지를 확인합니다.

PC의 TCP/IP 설정이 완료된 후 ipTIME에서 자동으로 IP 주소를 부여 받는지 확인하기 위해서는 윈도우를 설정하기 전에 PC와 ipTIME을 LAN 케이블로 연결하고 ipTIME을 켜두어야 합니다.

- 윈도우 아이콘 버튼을 클릭한 후 메뉴에서 제어판을 선택합니다.
- 제어판의 **네트워크 및 인터넷** 아이콘을 클릭합니다.



<네트워크 및 인터넷 클릭>

- 네트워크 및 인터넷 연결에서 **네트워크 및 공유 센터** 아이콘을 클릭합니다.



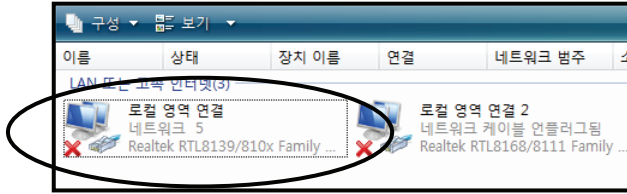
<네트워크 및 공유 센터 클릭>

- 네트워크 연결 관리를 클릭합니다.



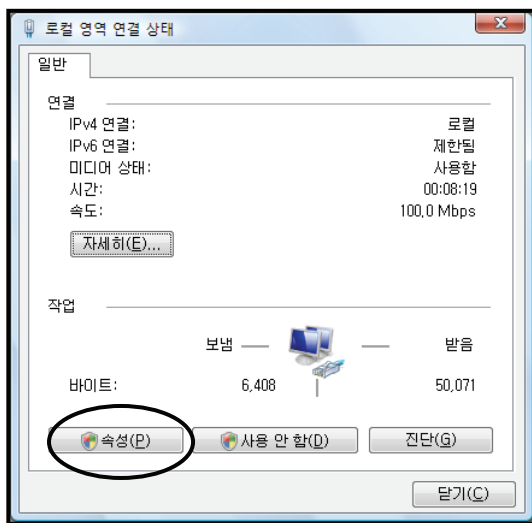
<네트워크 연결 관리 클릭>

- 네트워크 연결에서 **로컬 영역 연결** 을 더블 클릭하여 선택합니다.



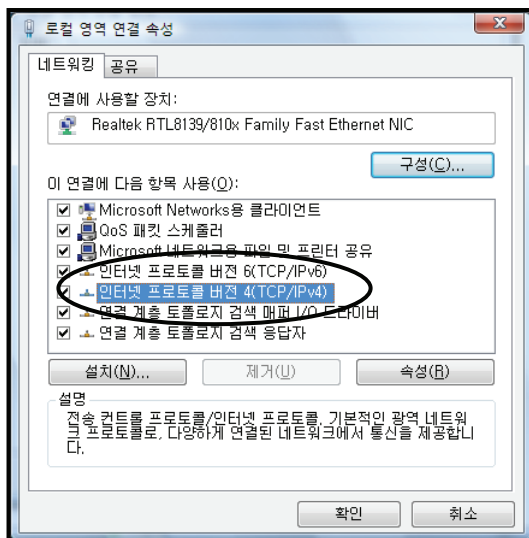
<로컬 영역 연결 더블 클릭>

- 로컬 영역 연결 상태에서 **속성**을 클릭하여 선택합니다.

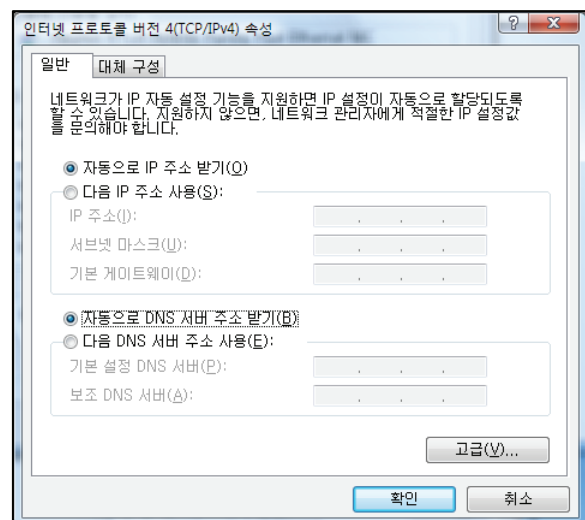


<속성 클릭>

- 인터넷 프로토콜 (TCP/IP)를 더블 클릭하여 선택하고 자동으로 IP 주소 받기와 자동으로 DNS 서버 주소 받기를 선택합니다.

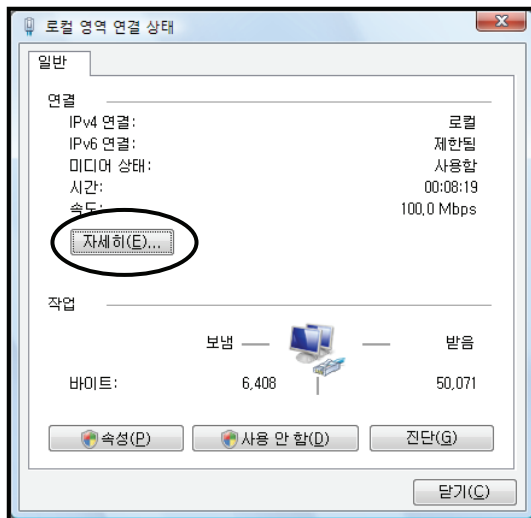


<TCP/IP 더블 클릭>



<자동 선택 후 확인 클릭>

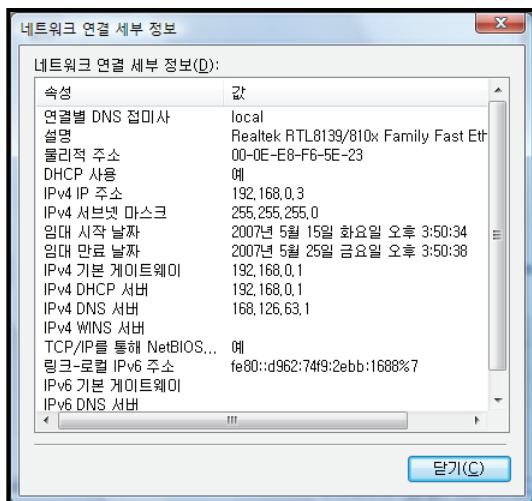
- 설정이 완료된 뒤 확인 버튼을 클릭하고 로컬 영역 연결 속성 창도 모두 닫아 줍니다.
- TCP/IP 설정을 완료하면 ipTIME에서 IP 주소를 자동으로 할당합니다. 자동할당을 위해서 PC와 ipTIME이 LAN 케이블로 연결되어야 합니다. 만일 케이블을 연결하지 않았다면 케이블을 연결한 뒤 PC를 다시 시작합니다.
- IP 주소 자동 할당 확인은 로컬 영역 연결 상태 창에서 **자세히** 버튼을 클릭하면 확인할 수 있습니다.



<자세히 클릭>

- **자세히** 버튼을 클릭하면 아래 그림과 같이 자동 할당된 IP 주소, 서브넷 마스크, 게이트웨이 등을 확인합니다.

[참고] ipTIME에 연결된 모든 PC는 각각 다른 IP 주소를 할당 받게 됩니다.



<IP 주소 확인>

IP Address : 192.168.0.2~254
Subnet Mask : 255.255.255.0
Default Gateway : 192.168.0.1

[참고] PC의 IP 주소가 정상적으로 자동 할당되지 않는다면 다음 사항을 확인한 뒤 PC를 재시작하여 IP주소가 할당되는지 확인합니다.

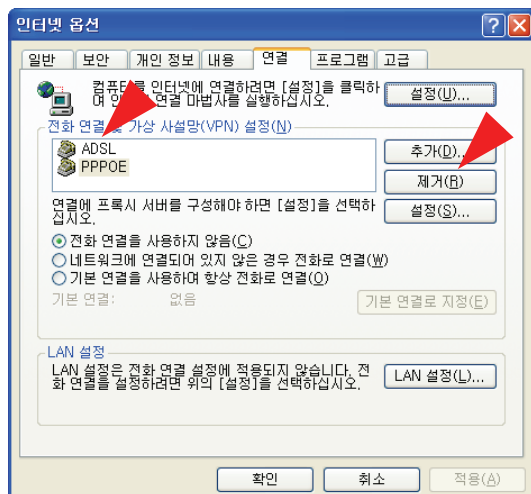
- PC와 ipTIME사이의 LAN 케이블 연결
- TCP/IP의 설정 내용 확인
- ADSL 접속 프로그램(광대역 연결 아이콘)의 제거 여부

위의 사항을 확인하여도 IP 주소가 정상적으로 자동 할당되지 않는다면 당사 홈페이지 (<http://www.iptime.co.kr>)를 참고하여 IP 주소 수동 설정 방법으로 IP 주소를 설정하거나 ipTIME 고객센터(070-7018-1199)에 문의하시기 바랍니다.

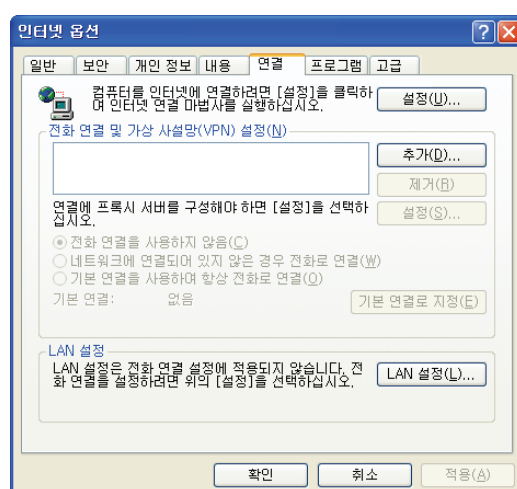
PC 설정을 완료한 뒤 인터넷을 사용하기 위해서는 3장의 내용을 참고하여 ipTIME의 WAN 포트를 인터넷에 연결 설정합니다. 인터넷 연결 설정은 공유기에서 이루어지는 것이므로 모든 PC에서 설정할 필요는 없이 한번만 설정하며, 설정 후 설정 저장을 해주시기 바랍니다

[참고] ADSL 사용시 인터넷 접속 프로그램 삭제 방법 (windows 98/ME)

- PPPoE 연결방식의 경우 Internet Explorer 실행시 접속프로그램의 자동실행으로 설정 화면이 나오지 않는 경우가 발생합니다. 이러한 경우 반드시 자동 실행되게 하는 연결 아이콘을 삭제하셔야 합니다.
- ADSL의 PPPoE 연결방식 사용자의 경우 프로그램추가/삭제에서 접속프로그램이 삭제되지 않았거나 프로그램을 찾기 어려울 경우 Internet Explorer의 **[도구] >> [인터넷 옵션] >> [연결]**에서 **[전화 연결 및 가상 사설망]**의 연결아이콘을 "제거"하여 줍니다



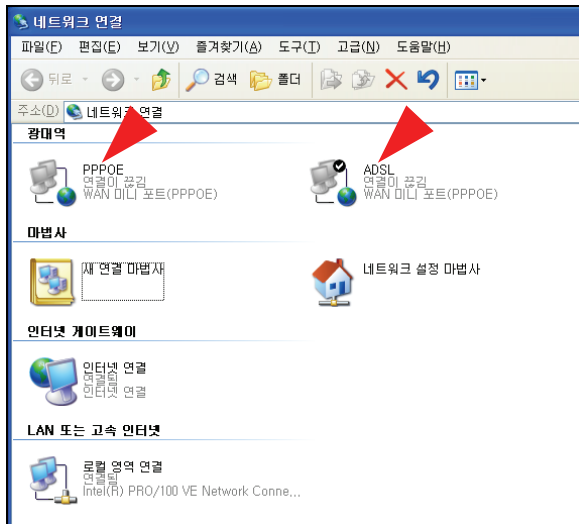
<ADSL의 연결 아이콘이 있는경우>



<전화접속 아이콘을 모두 삭제한 화면>

[참고] ADSL 사용시 Windows XP 광대역 연결 삭제 방법

- 바탕화면의 **시작** - **제어판** - **네트워크 연결**을 더블 클릭하여 나타나는 네트워크 연결 창에서 광대역에 추가되어있는 아이콘을 마우스 오른쪽 클릭 "삭제"합니다.
삭제되지 않을 경우 마우스 오른쪽 클릭하여 "연결 끊기"를 클릭하신 후 "삭제"합니다.



<광대역의 PPPoE연결 아이콘 화면>

2장 웹 설정 화면 이용하기

2.1 ipTIME 웹 서버 접속

- ipTIME 웹 서버에 접속하여 관련된 설정을 변경하거나 동작 상태를 확인할 수 있습니다. ipTIME 의 웹 설정 화면은 내부에 내장된 웹 서버를 이용하는 것이므로 인터넷이 연결되어 있지 않아도 접속할 수 있습니다.

- 웹 설정 화면에 접속하기 위해서는  Internet Explorer를 실행하여, 주소란에 ipTIME의 주소인 192.168.0.1을 입력합니다.

주소(D) http://192.168.0.1

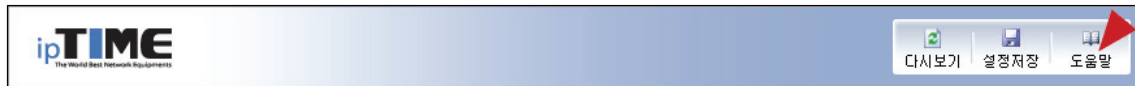
- ipTIME에 접속되면 아래 그림과 같은 화면이 표시되며 이때 **관리도구** 버튼을 클릭하면 ipTIME 웹 설정 화면으로 접속됩니다.



<웹 설정 화면>

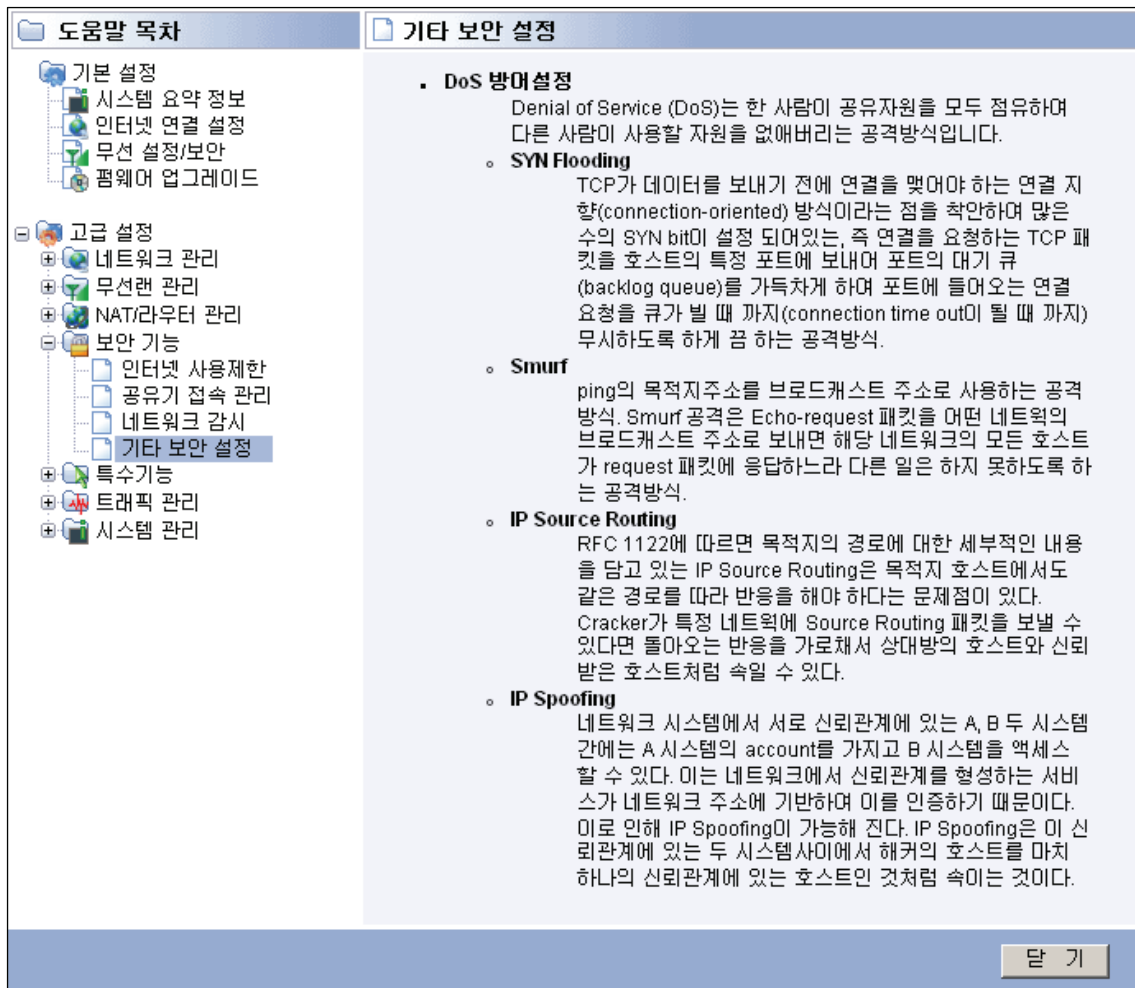
2.2 도움말 기능

- ipTIME 은 모든 기능에 대한 도움말을 내장하고 있습니다. ipTIME 웹 설정 화면의 우측 상단의 도움말을 클릭하면 해당 웹 설정 화면에 대한 자세한 도움말을 볼 수 있습니다.



<웹 설정 화면 우측 상단의 도움말 메뉴>

- 도움말 화면 좌측에는 전체 도움말의 목차가 링크되어 있으므로 필요한 경우 목차를 클릭하면 현재 화면 이외의 다른 기능에 대한 도움말도 확인할 수 있습니다.



<ipTIME 도움말 화면>

2.3 설정 저장 기능

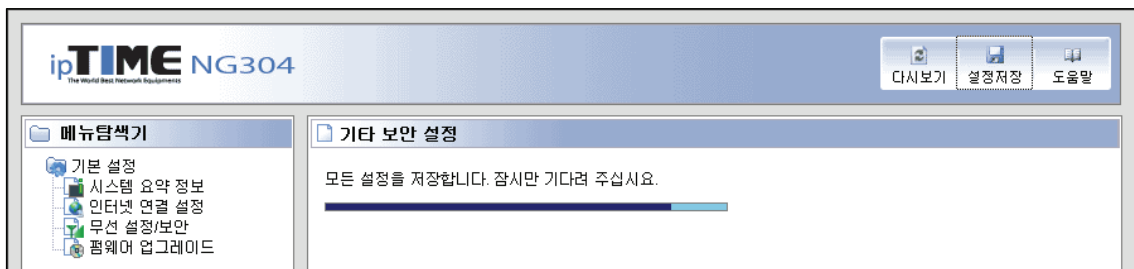
- ipTIME 웹 설정 화면으로 설정 변경된 내용은 설정 저장을 하여야 영구적으로 저장됩니다. 설정 저장을 하지 않으면 변경된 설정 내용은 공유기의 전원을 OFF하면 모두 지워집니다. 설정 저장을 위해서는 웹 설정 화면 우측 상단의 설정 저장 메뉴를 클릭합니다.



<웹 설정 화면 우측 상단의 설정 저장 메뉴>

- 설정저장 메뉴를 클릭하면 확인 창이 표시됩니다.

이때 확인을 클릭하면 아래 그림과 같이 설정저장 중임을 알리는 화면이 표시된 뒤 모든 설정 내용이 공유기 내부의 비휘발성 메모리에 기록됩니다.



<설정 저장을 알리는 화면 메시지 내용>

3장 설정 마법사로 인터넷 연결

- 본 3장에서는 ipTIME을 인터넷에 연결하는 방법에 대해서 설명합니다. 인터넷 연결 설정은 내장된 웹 설정화면에 접속하여 이루어집니다. 그러므로 인터넷 연결 설정은 ipTIME과 연결된 PC 중 한 곳에서 한번만 실행하면 됩니다.
- ipTIME에 내장된 웹 서버에 접속하기 위해서는 PC를 정상적으로 설정하여야 합니다. PC의 설정 방법에 대해서는 본 설명서 1장 참고하시거나, 제공되는 ‘ipTIME 설치도우미’를 이용하시면 됩니다.
- 인터넷 연결 설정은 ipTIME에 내장된 마법사를 이용하며, 자동 또는 수동 설정이 가능합니다. 3장에서는 이 마법사를 이용하여 인터넷 설정을 진행하는 방법을 설명합니다.
- 1장에서 3장까지의 내용에 따라 PC와 ipTIME의 설정을 완료하면 ipTIME과 연결된 PC에서 인터넷 사용이 가능합니다.
- 마법사를 사용하지 않고 인터넷 연결 설정을 진행하시려면 “5.2장 인터넷 연결 설정”을 참고합니다.
- 케이블 모뎀 방식의 인터넷 서비스 환경일 경우, 본 사용 설명서 1장을 진행하신 뒤, 모뎀과 공유기의 전원을 모두 끄고, 먼저 모뎀을 켜서 약 1분 후에 링크가 잡히면, 공유기의 전원을 켜주시면 별도의 설정 없이도 인터넷 연결이 이뤄질 수 있습니다.
 - 모뎀의 링크가 잡히면 CABLE, ONLINE, SYNC등의 램프는 점멸하다가 켜지게 됩니다.
 - 사용 환경에 따라 바로 연결이 되지 않을 수 있으며, 본 3장의 내용을 진행합니다.

3.1 ipTIME 웹 서버 접속

- ipTIME에 내장된 웹 서버는 인터넷이 연결되어 있지 않아도 접속할 수 있습니다.

웹 서버에 접속하기 위해서는  Internet Explorer를 실행하여, 주소란에 ipTIME의 주소인 192.168.0.1을 입력합니다.

주소(D)	http://192.168.0.1
-------	--------------------

- ipTIME에 접속되면 아래 그림과 같은 화면이 표시되며 이때 **설정마법사** 버튼을 클릭하면 마법사를 시작합니다.



<웹 설정 화면>

3.2 ipTIME 설정 마법사 실행

- ipTIME 초기화면에서 설정 마법사 버튼을 클릭하여 아래 그림과 같이 마법사를 시작합니다.

인터넷 연결 마법사를 시작합니다.
마법사를 실행시킬 방법을 선택하십시오.

☒ 자동으로 인터넷 연결을 검색하여 설정합니다.
인터넷 연결 방법을 자동으로 감지하여 설정합니다.
동적IP(DHCP) 또는 PPPoE 방식을 감지할 수 있습니다.

☐ 수동으로 인터넷 연결을 설정합니다.
모든 인터넷 연결을 수동으로 설정하실 수 있습니다.

다음 >

- 인터넷 회선을 확실히 알고 있는 경우 수동을 선택하며 인터넷 회선의 종류가 불확실한 경우 자동으로 선택하고 **다음** 버튼을 클릭합니다.
- 고정 IP 주소 서비스 사용자의 경우 자동 검색을 통하여 인터넷 설정을 할 수 없으므로 수동으로 인터넷 연결을 설정한 후 사용하여야 합니다.

인터넷 회선 선택 기준

유 형	내 용
동적 IP 주소	FTTH, 광랜 서비스 VDSL 서비스 ADSL이나 접속프로그램을 사용하지 않는 서비스 (IP-ADSL) 케이블 모뎀 서비스
PPPoE 방식	ADSL이며 접속시 사용자 이름과 암호를 입력하는 서비스 Aceman pro, WINPoET 등의 접속 프로그램 사용 XP의 경우 내장 광대역 접속 사용
고정 IP 주소	인터넷 서비스사로부터 지정된 IP 주소 할당 사용

3.3 자동 검색에 의한 PPPoE 연결 예

Aceman Pro, WinPOET, XP 광대역 접속 프로그램등을 사용하는 PPPoE 서비스 방식의 ADSL 환경에서 사용하는 경우 아래 순서로 인터넷 설정이 자동 진행됩니다.

[1] 자동 검색을 선택한 후 **다음** 버튼을 클릭합니다.

인터넷 연결 마법사를 시작합니다. 마법사를 실행시킬 방법을 선택하십시오.
☒ 자동으로 인터넷 연결을 검색하여 설정합니다. 인터넷 연결 방법을 자동으로 감지하여 설정합니다. 동적IP(DHCP) 또는 PPPoE 방식을 감지할 수 있습니다.
☐ 수동으로 인터넷 연결을 설정합니다. 모든 인터넷 연결을 수동으로 설정하실 수 있습니다.
다음 >

[2] WAN포트 연결 및 모뎀에 대한 내용 확인하시고 **다음** 버튼을 클릭합니다.

WAN포트 연결 성공 - 모뎀 재시작
WAN포트가 정상적으로 연결되어 있습니다. FTTH, 광랜등의 서비스처럼 벽에서 직접 인터넷선(랜선)이 나오는 경우는, '다음' 버튼을 눌러 계속 진행합니다. ADSL/VDSL/케이블모뎀 서비스방식일 경우는 모뎀의 전원을 껐다 켜줍니다. 일정 시간(최대 5분 이내)이 지난 후, 모뎀의 Link/Sync/Online등의 LED의 상태를 확인합니다. 해당 LED가 정상적으로 켜져 있으면, '다음' 버튼을 눌러 계속 진행합니다. * 해당 LED가 지속적으로 깜박거리면, 인터넷 서비스 제공업체에 문의합니다.
< 이 전 다음 >

[3] 인터넷 검색 중 화면이 나오는 동안 기다립니다.

인터넷 연결 검색 중

인터넷 연결을 검색하고 있습니다.
 검색을 마친 후에는 자동으로 검색 결과를 보여줍니다.
 이 과정은 최대 2분까지 소요될 수 있습니다.

< 이 전

다음 >

[4] PPPoE로 검색된 경우 사용자 계정과 암호를 입력하고 **다음** 버튼을 클릭합니다.

PPPoE 방식 검색됨
 사용자 계정 및 암호 입력

PPPoE를 사용하는 ADSL 방식의 인터넷 연결이 검색되었습니다.
 이 연결 방식은 인터넷 서비스 제공업체로부터 부여받은 사용자 계정 및 암호가 필요합니다.
 사용자 계정 및 암호를 정확히 입력한 후 '다음' 버튼을 클릭합니다.

사용자 계정

사용자 암호

사용자 계정 및 암호를 분실하였을 경우에는 인터넷 서비스 제공업체로 문의합니다
 KT : 국번없이 100
 하나로통신 : 국번없이 106
 (하나로 통신에서는 기본계정으로 사용자이름:hanaro@hanaro, 암호:1 을 제공하고있습니다)

< 이 전

다음 >

- 잘못된 암호/계정이라는 메시지가 나오는 경우 서비스 회사에 사용자 계정과 암호를 확인하여 다시 입력합니다.
- 정확한 암호/계정을 입력하여도 잘못된 암호/계정이라는 메시지가 나오면 12.5장을 참고하여 ipTIME을 공장 초기화한 후 다시 진행하여 보시기 바랍니다.

[5] 인터넷이 연결되면 할당 받은 IP 주소가 표시되며, **설정 저장 후 마법사 종료** 버튼을 클릭하여 마법사를 종료합니다.

인터넷 연결 성공
PPPoE 방식

PPPoE방식으로 인터넷에 연결되었습니다.
할당된 IP정보는 아래와 같습니다.

외부 IP 주소	61.77.128.253
서브넷 마스크	255.255.255.255
기본 게이트웨이	61.77.128.253
기본 DNS 서버	168.126.63.1
보조 DNS 서버	168.126.63.2

현재의 인터넷 설정을 적용하려면 "설정 저장 후 마법사 종료" 버튼을 클릭합니다.

마법사 재실행

설정 저장 후 마법사 종료

3.4 자동 검색에 의한 동적 IP 연결 예

동적 IP 방식 (DHCP 방식)의 서비스인 FTTH, 광랜, 케이블 모뎀, VDSL, LAN, IP-ADSL에 연결된 경우 아래 순서로 인터넷 설정이 자동 진행됩니다.

[1] 자동 검색을 선택한 후 **다음** 버튼을 클릭합니다.

인터넷 연결 마법사를 시작합니다.
 마법사를 실행시킬 방법을 선택하십시오.

☒ 자동으로 인터넷 연결을 검색하여 설정합니다.
 인터넷 연결 방법을 자동으로 감지하여 설정합니다.
 동적IP(DHCP) 또는 PPPoE 방식을 감지할 수 있습니다.

☐ 수동으로 인터넷 연결을 설정합니다.
 모든 인터넷 연결을 수동으로 설정하실 수 있습니다.

다음 >

[2] WAN포트 연결 및 모뎀에 대한 내용을 확인하시고 **다음** 버튼을 클릭합니다.

WAN포트 연결 성공 - 모뎀 재시작

WAN포트가 정상적으로 연결되어 있습니다.

 FTTH, 광랜 등의 서비스처럼 벽에서 직접 인터넷선(랜선)이 나오는 경우는,
 '다음' 버튼을 눌러 계속 진행합니다.

ADSL/VDSL/케이블모뎀 서비스방식일 경우는 모뎀의 전원을 껐다 켜줍니다.
 일정 시간(최대 5분 이내)이 지난 후, 모뎀의 Link/Sync/Online 등의 LED의 상태를 확인합니다.
 해당 LED가 정상적으로 켜져 있으면, '다음' 버튼을 눌러 계속 진행합니다.

* 해당 LED가 지속적으로 깜박거린다면, 인터넷 서비스 제공업체에 문의합니다.

< 이 전 다음 >

[3] 인터넷 검색 중 화면이 나오는 동안 기다립니다.

인터넷 연결 검색 중

인터넷 연결을 검색하고 있습니다.
 검색을 마친 후에는 자동으로 검색 결과를 보여줍니다.
 이 과정은 최대 2분까지 소요될 수 있습니다.

< 이 전

다음 >

[4] 동적 IP 방식으로 인터넷이 검색되면 아래 그림과 같이 설정이 종료되며, **설정 저장 후 마법사 종료** 버튼을 클릭하여 마법사를 종료합니다.

인터넷 연결 성공
 동적IP(DHCP) 방식

동적IP방식(DHCP)으로 인터넷에 연결되었습니다.
 할당된 IP정보는 아래와 같습니다.

외부 IP 주소	192.168.11.121
서브넷 마스크	255.255.255.0
기본 게이트웨이	192.168.11.254
기본 DNS 서버	168.126.63.1
보조 DNS 서버	168.126.63.2

현재의 인터넷 설정을 적용하려면 "설정 저장 후 마법사 종료" 버튼을 클릭합니다.

마법사 재실행

설정 저장 후 마법사 종료

[참고]

- 동적 IP 방식을 자동으로 검색하는 경우 자동 검색을 실행한 PC의 하드웨어 주소(MAC Address)가 해당 WAN 포트에 자동 복사됩니다.
- PC의 하드웨어 주소(MAC Address)란 PC에 설치되어 있는 LAN 카드의 고유 번호이며, 동적 IP 방식 서비스의 경우 일부 인터넷 서비스 회사에서 하드웨어 주소를 확인하여 한 대의 PC만 인터넷을 사용할 수 있도록 하고 있습니다. 이와 같은 경우 PC의 하드웨어 주소를 IP 공유기로 복사하면 하드웨어 주소 검사에 따른 제약 없이 IP 공유기를 사용할 수 있습니다.
- WAN 포트에 모뎀이나 랜방식의 회선이 아닌 IP공유기의 UTP-케이블을 연결하신 경우 검색 실패로 나옵니다.

이러한 경우에는 5장의 5.2.1 동적 IP 방식 설정의 그림과 같이 “사설 IP 할당 허용하기”를 반드시 체크하시고 하단의 적용을 눌러주시면 IP공유기의 연결도 사용할 수 있습니다.

3.5 수동 설정을 이용한 인터넷 연결 설정

마법사를 이용한 자동 인터넷 검색에 실패하였거나 인터넷 서비스의 종류를 정확히 알고 있는 경우, 그리고 인터넷 서비스 회사로부터 할당 받은 고정 IP 주소를 사용하는 My IP, Multi IP 등과 같은 서비스를 사용하는 경우 수동 설정을 이용하여 인터넷을 연결합니다.

[1] 수동 설정을 선택한 후 **다음** 버튼을 클릭합니다.

인터넷 연결 마법사를 시작합니다.
 마법사를 실행시킬 방법을 선택하십시오.

☐ 자동으로 인터넷 연결을 검색하여 설정합니다.
 인터넷 연결 방법을 자동으로 감지하여 설정합니다.
 동적IP(DHCP) 또는 PPPoE 방식을 감지할 수 있습니다.

☒ 수동으로 인터넷 연결을 설정합니다.
 모든 인터넷 연결을 수동으로 설정하실 수 있습니다.

다음 >

[2] 고정 IP 방식을 선택한 후 **다음** 버튼을 클릭합니다.

인터넷 연결방식 선택

☐ 동적으로 IP를 할당받는 방법(DHCP)
 FTTH,광랜,케이블모뎀,VDSL,IP ADSL,LAN방식등의 서비스에 적합합니다.
 이 방식은 DHCP 프로토콜을 이용하여 IP를 동적으로 할당받는 방법입니다.

☐ 사용자 계정과 암호를 필요로 하는 인터넷 연결(PPPoE)
 ADSL모뎀(PPPoE지원) 사용시 적합한 방식입니다.
 이 방식은 PPPoE 프로토콜을 이용하여 인터넷에 연결합니다.
 사용자 계정 및 암호는 인터넷 서비스 회사로부터 제공받습니다.

☒ 고정 IP를 사용하는 인터넷에 연결(Static IP)
 인터넷 서비스 제공업체로부터 할당받은 고정IP를 설정하는 방식입니다.
 IP주소,서브넷 마스크,게이트웨이,DNS 등의 주소를 직접 입력합니다.

< 이 전 다음 >

- 고정 IP 서비스 방식의 경우 인터넷 서비스 회사에서 입력 받은 IP 주소와 게이트웨이 DNS 주소를 입력한 뒤 **다음** 버튼을 클릭합니다..

고정 IP를 사용하는 인터넷에 연결(Static IP)
 IP주소, 서브넷마스크, 게이트웨이, DNS 서버를 입력

외부 IP 주소	61	77	128	253
서브넷 마스크	255	255	255	0
기본 게이트웨이	61	77	128	1
기본 DNS서버	168	126	63	1
보조 DNS서버	168	126	63	2

< 이 전
다음 >

- 위에 입력한 IP주소 값은 임의 IP주소 값이므로 PC에 IP를 수동으로 입력한 값이나 인터넷 서비스 업체에서 준 계약서의 IP주소 값을 넣어 주셔야 합니다.

인터넷 연결 설정 확인

설정 될 내용이 다음과 같습니다.

연결방식	고정IP 방식
외부 IP 주소	61.77.128.253
서브넷 마스크	255.255.255.0
기본 게이트웨이	61.77.128.1
기본 DNS서버	168.126.63.1
보조 DNS서버	168.126.63.2

현재의 인터넷 설정을 적용하려면 "설정 저장 후 마법사 종료" 버튼을 클릭합니다.

< 이 전
설정 저장 후 마법사 종료

[3] PPPoE 방식을 선택한 후 **다음** 버튼을 클릭합니다.

인터넷 연결방식 선택

☐ 동적으로 IP를 할당받는 방법(DHCP)
 FTTH,광랜,케이블모뎀,VDSL,IP ADSL,LAN방식등의 서비스에 적합합니다.
 이 방식은 DHCP 프로토콜을 이용하여 IP를 동적으로 할당받는 방법입니다.

☒ 사용자 계정과 암호를 필요로 하는 인터넷 연결(PPPoE)
 ADSL모뎀(PPPoE지원) 사용시 적합한 방식입니다.
 이 방식은 PPPoE 프로토콜을 이용하여 인터넷에 연결합니다.
 사용자 계정 및 암호는 인터넷 서비스 회사로부터 제공받습니다.

☐ 고정 IP를 사용하는 인터넷에 연결(Static IP)
 인터넷 서비스 제공업체로부터 할당받은 고정IP를 설정하는 방식입니다.
 IP주소,서브넷 마스크,게이트웨이,DNS 등의 주소를 직접 입력합니다.

- 사용자 계정 및 암호를 필요로 하는 PPPoE ADSL 방식의 경우 서비스 회사에서 부여 받은 사용자 계정 및 암호를 입력하고 **다음** 버튼을 클릭합니다.

사용자 계정과 암호를 필요로 하는 인터넷 연결(PPPoE)
 사용자 계정 및 암호 입력

사용자 계정 및 암호는 인터넷 서비스 제공 업체로부터 제공받습니다.

사용자 계정

사용자 암호

사용자 계정 및 암호를 분실하였을 경우에는 인터넷 서비스 제공업체로 문의합니다
 KT : 국번없이 100
 하나로통신 : 국번없이 106
 (하나로 통신에서는 기본계정으로 사용자이름:hanaro@hanaro, 암호:1 을 제공하고있습니다)

- 잘못된 암호/계정이라는 메시지가 나오는 경우 서비스 회사에 사용자 계정과 암호를 확인하여 다시 입력합니다.
- 정확한 암호/계정을 입력하여도 잘못된 암호/계정이라는 메시지가 나오면 12.5장을 참고하여 ipTIME을 공장 초기화한 후 다시 진행하여 보시기 바랍니다.

인터넷 연결 설정 확인

설정 될 내용이 다음과 같습니다.

연결방식	사용자계정 및 암호입력 방식(PPPoE)
사용자 계정	coolefm
사용자 암호	*****

현재의 인터넷 설정을 적용하려면 "설정 저장 후 마법사 종료" 버튼을 클릭합니다.

[< 이 전](#)[설정 저장 후 마법사 종료](#)

[4] 동적 IP 방식을 선택한 후 **다음** 버튼을 클릭합니다.

인터넷 연결방식 선택

☒ **동적으로 IP를 할당받는 방법(DHCP)**
FTTH,광랜,케이블모뎀,VDSL,IP ADSL,LAN방식등의 서비스에 적합합니다.
이 방식은 DHCP 프로토콜을 이용하여 IP를 동적으로 할당받는 방법입니다.

☐ **사용자 계정과 암호를 필요로 하는 인터넷 연결(PPPoE)**
ADSL모뎀(PPPoE지원) 사용시 적합한 방식입니다.
이 방식은 PPPoE 프로토콜을 이용하여 인터넷에 연결합니다.
사용자 계정 및 암호는 인터넷 서비스 회사로부터 제공됩니다.

☐ **고정 IP를 사용하는 인터넷에 연결(Static IP)**
인터넷 서비스 제공업체로부터 할당받은 고정IP를 설정하는 방식입니다.
IP주소,서브넷 마스크,게이트웨이,DNS 등의 주소를 직접 입력합니다.

< 이 전
 다음 >

- 정상 연결이 안될 경우 모뎀에서 이전 연결한 PC의 하드웨어 주소(MAC Address)를 저장하고 있어 연결이 되지 않는 경우가 있습니다.

동적으로 IP를 할당받는 방법(DHCP)
WAN포트의 MAC 주소 입력

WAN포트의 MAC 주소를 변경합니다.

☒ 현재 접속 되어 있는 PC의 MAC 주소를 자동으로 입력

☐ PC의 MAC 주소를 수동으로 입력
 - - - - -
 공유기를 사용하지 않고 인터넷을 사용했던 PC의 MAC 주소를 입력합니다.

☐ MAC 주소를 변경하지 않음.

☒ 사설 IP할당을 허용합니다.

< 이 전
 다음 >

- 정상 연결이 안될 경우 모뎀에서 이전 연결한 PC의 하드웨어 주소(MAC Address)를 저장하고 있어 연결이 되지 않는 경우가 있습니다.
 이러한 경우에는 모뎀과 공유기를 꺼주시고 모뎀부팅 후(약 1~2분) 공유기를 부팅하시고 (10초 후) 위 설정을 다시 시작 시작해 보시기 바랍니다.

인터넷 연결 설정 확인

설정 될 내용이 다음과 같습니다.

연결방식	동적IP 방식-DHCP사용
WAN포트의 MAC 주소	접속된 PC의 MAC 주소 : 00-13-8F-43-F2-10
사설IP할당	허용함

현재의 인터넷 설정을 적용하려면 "설정 저장 후 마법사 종료" 버튼을 클릭합니다.

[< 이 전](#)[설정 저장 후 마법사 종료](#)

4장 무선랜 연결 및 설정

4장은 무선 AP기능이 제공되는 ipTIME 유무선 공유기 제품에서만 해당되는 내용입니다.

- 제4.1장에서는 ipTIME의 무선 네트워크 구성 방법을 설명합니다.
- 제4.2장에서는 무선 PC를 ipTIME에 연결하는 방법을 설명합니다.
- 4장의 무선 기능을 사용하기 위해서는 1~3장의 설정을 완료하여야 합니다.

4.1 무선 네트워크 구성

ipTIME에 내장된 AP를 사용하여 무선 네트워크를 구축하기 위해서는 AP를 사용 환경에 맞게 설정하여야 합니다. AP 설정은 무선 연결 마법사를 이용하거나 공유기 설정 화면에서 설정할 수 있습니다.

4.1.1은 무선 설정 마법사를 이용하는 방법, 4.1.2은 무선 네트워크 구성에 필요한 개념을 설명합니다.

ipTIME 으로 무선 네트워크 구성을 위한 AP 설정은 아래 표에 해당하는 값을 결정하는 것이며 마법사를 이용하면 간단하게 설정할 수 있으며 공유기 설정 화면을 이용하면 보다 자세한 설정이 가능합니다.

내용	기본값	설명
SSID	iptime	무선 네트워크 구성 시 구성되는 네트워크 이름
SSID 알림	ON	무선 네트워크의 이름을 단말 장치에 알려주는 기능
채널	6	무선 네트워크에서 사용되는 채널 (대한민국 : 1~13 중 선택) 국가 선택에 따라 채널 범위가 변경됨
인증 방법	자동	AP에 단말 등록 시 인증 절차를 결정함
암호화 방법	사용 안함	AP와 단말 Data 통신 시 사용되는 WEP Key 값을 결정
MAC 주소 인증	모두 허용	AP에 단말 등록 시 등록된 MAC 주소의 단말만 허용

IEEE 802.11b/g의 무선 네트워크에 대한 지식이 부족한 경우 무선 네트워크 설치 전 4.1.2의 내용을 먼저 읽고 무선 AP 설정을 진행하면 도움이 됩니다.

4.1.1 무선 설정 마법사를 이용한 무선 네트워크 구성

무선에 대한 설정 값이 바뀌기 때문에 무선 연결이 끊어질 수 있으므로 반드시 공유기와 유선으로 연결된 PC에서 설정하시기 바랍니다

- 공유기에 유선랜으로 연결된 PC에서  Internet Explorer를 실행합니다.
- 주소”란에 아래 그림과 같이 공유기의 IP 주소인 “192.168.0.1” 을 입력하고 “Enter” 키를 누릅니다.

주소(D)	http://192.168.0.1
-------	--------------------

- ipTIME에 접속되면 아래 그림과 같은 화면이 표시되며 이때 **무선마법사** 버튼을 클릭하면 마법사를 시작합니다.



<웹 설정 화면>

[1] 무선 설정 마법사를 시작합니다. **다음** 버튼을 클릭합니다.

무선 설정 마법사 시작합니다.

무선 설정 마법사를 실행하여 무선관련 설정을 손쉽게 할 수 있습니다.
무선 마법사를 계속 진행하려면 '다음' 버튼을 클릭합니다.

주의] 무선으로 연결된 PC에서 마법사 실행 시 마법사의 진행이 원활하지 않을 수 있습니다.

다음 >

[2] 무선 네트워크를 구성할 국가를 선택하고 **다음** 버튼을 클릭합니다.

사용 국가 설정
 장비를 사용할 국가를 선택합니다.

무선랜 신호는 국가별로 사용할 수 있는 채널이 제한되어 있습니다.
사용하고자 하는 국가를 선택한 후 '다음' 버튼을 클릭합니다.

< 이 전 **다음 >**

- 대한민국을 선택하면 전파 관리법에 의하여 허용된 13개 채널을 사용할 수 있습니다.
- 미국을 선택한 경우 FCC 규정에 따라 11개, 일본의 경우 14개 채널을 사용할 수 있습니다.

[3] 구성하고자 하는 무선네트워크의 SSID 를 입력하고 다음 버튼을 클릭합니다.

네트워크 이름(SSID) 입력

네트워크 이름(SSID)은 무선 네트워크를 식별하기 위해 사용됩니다.
따라서, 주변의 다른 무선 네트워크 이름과 중복되지 않도록 설정할 것을 권장합니다.

'중복검사' 버튼을 클릭하여 네트워크 이름을 확인하십시오.
중복 검사가 완료되면 '다음' 버튼을 눌러 계속 진행합니다.
* 일부 특수한 경우에 동일한 네트워크 이름(SSID)을 사용할 수도 있습니다.

네트워크 이름(SSID) 입력

- SSID는 사용자가 원하는 문자열을 영문으로 입력합니다.
- 입력된 SSID 값은 AP를 통하여 무선으로 모든 단말기에 전달됩니다.

[4] 공유기는 인접한 무선 네트워크를 검색합니다.

무선 채널 설정

최적의 채널을 탐색한 후 선택합니다.

'최적의 채널 검색이 끝나면, '다음' 버튼을 눌러 계속 진행합니다.
* 다른 채널도 수동으로 설정할 수 있습니다.

주변의 무선 네트워크를 검색중입니다.
잠시만 기다리십시오.

45

- 무선 네트워크 검색이 완료되면 검색 결과를 표시하여 줍니다.
- 자동 검색된 최적의 채널을 선택 사용하기를 권장합니다.
- 사용하고자 하는 채널을 선택한 뒤 **다음** 버튼을 클릭합니다.

무선 채널 설정
 최적의 채널을 탐색한 후 선택합니다.

'최적의 채널' 검색이 끝나면, '다음' 버튼을 눌러 계속 진행합니다.
 * 다른 채널도 수동으로 설정할 수 있습니다.

최적의 채널 검색


채널7번 최적의 채널로 검색됨


채널8번 (1개의 AP가 사용중)
 사용중인 무선AP: wireless_devnet


채널9번 (1개의 AP가 사용중)
 사용중인 무선AP: labtest

< 이전

다음 >

[5] 입력된 채널과 SSID 를 확인한 후 **다음** 버튼을 클릭합니다.

설정 내용 확인

아래의 설정내용을 확인합니다.

사용국가	대한민국 (1번 ~ 13번)
무선채널	7
네트워크이름(SSID)	iptime

설정 내용을 확인 후, '다음' 버튼을 클릭하여 무선 보안 설정을 진행합니다.

< 이전

다음 >

[6] 무선 보안 방식을 선택 후 **다음** 버튼을 클릭합니다.

무선 보안 설정
 무선 보안 방식을 선택합니다.

☒ **네트워크 키를 공유하는 보안 방식을 사용합니다.(WEP)**
 고전적인 암호화 방식으로 WPA 방식을 지원하지 않는 무선랜카드와 연결할 수 있습니다.

☐ **WPA 기반의 향상된 보안 방식(WPA-PSK)**
 802.11i에 정의된 표준 방식으로, WEP 보다 더욱 향상된 보안 방식입니다.

☐ **무선 보안을 사용하지 않음**
 외부에서 이 네트워크로의 침입을 막을 수 없고, 통신 중인 데이터가 쉽게 노출될 수 있습니다.

☐ **현재의 무선 보안 설정을 그대로 사용함**

< 이 전

다음 >

- WEP방식은 [7] 절차를 참조하세요
- WPA-PSK 방식은 [8] 절차를 참조하세요.
- 무선 보안을 사용하지 않는 경우 또는 현재 무선 보안 설정을 그대로 사용하는 경우에는 별도의 보안 설정 절차가 없습니다.

[7] WEP 방식을 선택한 경우

- 네트워크 키의 길이를 선택합니다.

네트워크 키 공유 방식
 네트워크 키의 길이를 선택합니다.

☒ **64 bit 길이의 네트워크 키를 사용하여 암호화 합니다.**

☐ **128 bit 길이의 네트워크 키를 사용하여 암호화 합니다.**

네트워크 키의 길이를 선택 후, '다음' 버튼을 클릭하여 계속 진행합니다.

< 이 전

다음 >

- 선택한 네트워크 키의 길이에 맞는 키 값을 입력합니다.

네트워크 키 입력

네트워크 키
 네트워크 키 확인
 네트워크 키는 정확히 5글자를 입력하여야 합니다.
 네트워크 키를 입력 후, '다음' 버튼을 클릭하여 계속 진행합니다.

< 이 전 다음 >

- 설정 내용을 확인한 후에, **설정 적용 후 마법사 마침** 버튼을 클릭합니다.

설정 내용 확인 및 적용

아래의 설정내용을 확인합니다.

사용국가	대한민국 (1번 ~ 13번)
무선채널	7
네트워크이름(SSID)	iptime
무선보안	공유 모드
암호화 방식	WEP

설정 내용을 확인 후, '설정 적용 후 마법사 마침' 버튼을 클릭하면
 모든 설정이 적용된 후 마법사가 자동으로 종료됩니다.

< 이 전 **설정 적용 후 마법사 마침**

[8] WPAPSK 방식을 선택한 경우

- TKIP 또는 AES 암호화 방식을 선택합니다.

WPA기반의 보안(WPAPSK)
암호화 방식을 선택합니다.

☒ **TKIP 방식**
WEP 보안 방식을 응용한 암호화 방식입니다.
11g를 지원하는 대부분의 무선 랜카드에서 지원됩니다.

☐ **AES 방식**
TKIP보다 강력한 새로운 암호화 방식입니다.
일부 무선 랜카드에서 지원되지 않을 수 있습니다.

암호화 방식을 선택 후, '다음' 버튼을 클릭하여 계속 진행합니다.

- 네트워크 키 값을 입력합니다.

네트워크 키 입력

네트워크 키

네트워크 키 확인

네트워크 키는 8글자 이상 입력하여야 합니다.

네트워크 키를 입력 후, '다음' 버튼을 클릭하여 계속 진행합니다.

- 설정 내용을 확인한 후에, **설정 적용 후 마법사 마침** 버튼을 클릭합니다.

설정 내용 확인 및 적용

아래의 설정내용을 확인합니다.

사용국가	대한민국 (1번 ~ 13번)
무선채널	7
네트워크이름(SSID)	iptime
무선보안	WPA PSK
암호화 방식	TKIP

설정 내용을 확인 후, '설정 적용 후 마법사 마침' 버튼을 클릭하면 모든 설정이 적용된 후 마법사가 자동으로 종료됩니다.

< 이 전
설정 적용 후 마법사 마침

[9] 무선 보안을 사용하지 않는 경우

설정 내용 확인 및 적용

아래의 설정내용을 확인합니다.

사용국가	대한민국 (1번 ~ 13번)
무선채널	7
네트워크이름(SSID)	iptime
무선보안	자동인증
암호화 방식	암호화 사용안함

설정 내용을 확인 후, '설정 적용 후 마법사 마침' 버튼을 클릭하면 모든 설정이 적용된 후 마법사가 자동으로 종료됩니다.

< 이 전
설정 적용 후 마법사 마침

4.1.2 무선 AP 설정에 필요한 개념

무선랜 표준 IEEE 802.11b/g

무선랜의 표준은 IEEE 라는 국제 표준화 기구의 표준을 따릅니다. 무선랜의 표준은 11Mbps 의 802.11b 표준과 54Mbps 의 802.11g 와 802.11a 표준이 있습니다. 802.11g 는 2.4GHz 의 주파수 대역을 사용하여 802.11b 와 상위 호환성이 있습니다. ipTIME 유무선 공유기는 802.11g AP 이므로 802.11g 는 물론 11Mbps 의 802.11b 장비의 연결도 가능합니다. 802.11a 표준은 5GHz 의 주파수를 사용하는 표준으로 802.11b/g 와 호환되지 않습니다.

무선랜 네트워크 구성 방법 (Infrastructure 모드, Ad-hoc 모드)

무선랜을 구성하는 방법은 Infrastructure 모드와 Ad-hoc 모드의 2 가지가 있습니다. Infrastructure 모드는 AP 를 이용하여 네트워크를 구성하는 방법으로 무선랜에 연결된 모든 단말들은 AP 에 접속되어 통신하는 방식으로 AP 에서 전체 통신을 관리하므로 안정성과 효율이 좋습니다. Ad-hoc 모드는 AP 없이 무선 랜 카드만을 이용하여 무선 네트워크를 구성하는 방법으로 안정성과 효율성이 떨어집니다. ipTIME 유무선 공유기를 사용하는 경우 무선 단말의 네트워크 모드를 Infrastructure 로 설정합니다.

SSID (Service Set Identifier, 네트워크 이름)

무선으로 구성되는 네트워크의 이름입니다. 무선 네트워크의 모든 단말과 AP 는 동일한 SSID 를 갖고 있어야 합니다. SSID 는 AP 에서 먼저 설정하며 AP 에 접속하고자 하는 단말기는 AP 와 동일한 SSID 를 입력하여야 합니다. 일반적으로 SSID 는 사용자가 임의로 결정하여 입력하면 됩니다. AP 는 자신의 SSID 를 모든 단말에게 알려줄 수도 있습니다. 이와 같은 경우 모든 단말에서 AP 존재를 쉽게 검색할 수 있는 장점이 있으나 원하지 않는 단말에서도 네트워크 존재가 파악되므로 보안에 문제가 발생할 수 있습니다. 이와 같은 경우 WEP 인증이나 MAC 인증으로 무선 보안을 설정하는 것이 좋습니다.

무선 채널

802.11b/g 표준은 2.4GHz 의 주파수를 14 개의 채널로 분리 사용하도록 규정합니다. 즉, 동일한 지역에서 조금씩 다른 주파수 14 개를 이용하여 별도의 무선 네트워크를 구축할 수 있습니다. 그러나 주파수 사용에 대한 법규가 국가마다 조금씩 달라서 사용할 수 있는 채널에 차이가 있습니다. 한국의 경우 13 개 채널을 사용할 수 있으며 미국/캐나다 등의 경우 11 개 채널, 일본의 경우 14 개 채널을 사용할 수 있도록 되어 있습니다.

무선 네트워크를 구축할 때에는 다른 AP 등에서 사용하지 않는 채널을 이용하여야 합니다. ipTIME 유무선 공유기의 무선 설정 마법사에는 채널 검색 기능이 포함되어 있어 사용하지 않는 채널을 쉽게 검색할 수 있습니다.

보안 및 암호화

무선 네트워크 표준안에서 제공하는 보안은 2 단계로 구성됩니다. 1 단계는 인증(Authentication)이며 2 단계는 WEP 암호화입니다. 1 단계 인증에서는 단말기가 공유기에 최초 통신을 시도할 때 단말기를 등록하여 향후 통신을 허가할 것인지를 결정하는 단계입니다. 2 단계 WEP 암호화에서는 이미 등록된 단말기가 통신을 할 때 전송되는 모든 데이터를 WEP key 를 이용하여 암호화 하는 것입니다.

Open System 의 경우, 별도의 인증 없이 단말을 AP 에 등록하며 Open System 을 선택하는 경우 일반적으로 통신 데이터에 대하여 WEP 암호화를 사용하지 않습니다.

Shared key 의 경우, WEP Key 에 따른 인증 절차를 거친 뒤 AP 에 단말이 등록되며 일반적으로 통신 데이터에 대해서 WEP 암호화를 사용합니다.

자동의 경우, WEP 입력 유무에 따라 적절한 인증과 데이터 암호화를 결정하는 방법입니다. ipTIME 유무선 공유기는 자동에 WEP 암호화를 사용하지 않는 것을 기본 값으로 하고 있습니다.

MAC 주소 인증

MAC 주소란 단말기 무선랜 카드가 갖고 있는 고유한 번호를 말합니다. ipTIME 유무선 공유기의 무선 MAC 주소 인증 기능은 등록된 MAC 주소를 갖는 무선 단말기의 AP 접속을 허용하거나 거부하는 기능입니다. 등록되지 않은 MAC 주소를 갖는 무선 단말기 AP 와 모든 통신이 거부됩니다. MAC 주소 인증을 통한 보안 관리를 이용하면 개별 단말기 사용자에게 WEP 비밀 번호 또는 SSID 값 등을 알려주지 않아도 되므로 관리자 입장에서는 편리하게 보안을 유지할 수 있습니다.

MIMO

MIMO 는 Multiple In Multiple Out 의 약자로 차세대 무선규격인 802.11n 에 적용되는 기술입니다. MIMO 기술을 적용한 ipTIME 유무선 공유기는 기존 802.11g 제품과 비교하여 무선 전송 속도 및 거리에서 50%이상의 성능 향상을 보여 줍니다.

4.2 무선 단말 연결 방법

일반적으로 노트북 또는 데스크탑 컴퓨터에 무선랜 카드를 설치하면 무선 환경 설정을 위한 유틸리티가 제공됩니다. Windows 95/98/ME/2000의 경우 유틸리티를 이용하여 단말의 무선 환경을 설정할 수 있으며 Windows XP의 경우 XP에 내장된 윈도우 자체 유틸리티를 이용하거나 혹은 Windows 95/98/ME/2000와 같이 제공되는 별도 유틸리티를 이용할 수 있습니다.

4.2.1에서는 95/98/ME/2000 환경에서 유틸리티를 이용하여 단말의 무선 환경을 설정하는 예를 보여주며 4.2.3에서는 XP에 내장된 윈도우 자체 유틸리티를 이용하는 예를 보여 줍니다.

사용자가 사용하는 무선랜 카드의 설치 및 유틸리티 설치의 구입한 무선랜 카드 설명서를 참조하거나 해당 무선랜 카드 제조/판매사에 문의합니다.

4.2.1 무선랜 카드 유틸리티를 이용한 무선 단말 연결

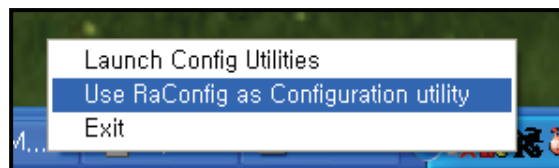
[참고] 무선랜 카드의 종류에 따라 유틸리티 프로그램의 구성 및 동작 방법이 다를 수 있으므로 자세한 유틸리티 사용 방법은 무선랜 카드 구입처에 문의합니다.

다음 예시는 ipTIME G054U의 무선 유틸리티를 이용한 접속 과정입니다.

- 윈도우 95/98/ME/2000의 경우 무선랜 카드와 같이 공급되는 유틸리티 프로그램을 실행합니다.
- 무선 유틸리티를 이용하여 ipTIME 공유기에 접속하는 방법입니다.
- 작업 표시줄 우측에 Ralink 아이콘을 더블 클릭합니다.
- “Use RaConfig as Configuration utility”를 클릭하여 Ralink utility를 실행합니다.

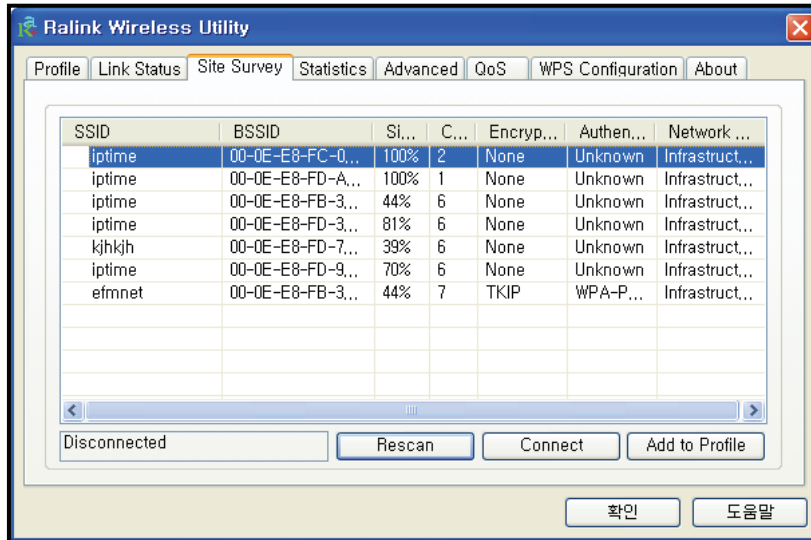


<Ralink 아이콘>



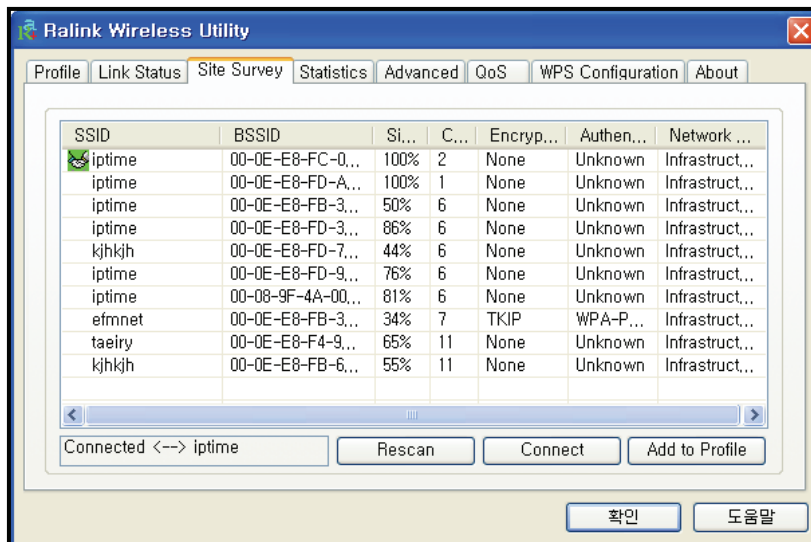
<Ralink utility 실행 하기>

- 무선랜 설정 화면은 아래 그림과 같습니다.
- Site Survey 탭 화면에서 각 AP의 정보를 확인 후 연결하고자 하는 SSID를 더블 클릭 합니다.



<Ralink utility 실행 화면>

- 선택한 SSID 좌측에 아이콘이 생기면 연결된 것을 확인 할 수 있습니다.



<연결된 SSID>

4.2.2 WEP 보안 사용

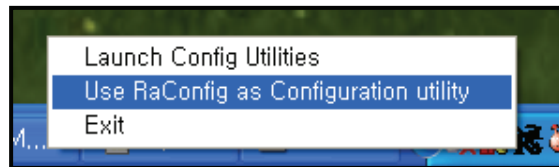
[참고]

WEP (Wired Equivalent Privacy): WEP은 유선랜에서 제공하는 것과 유사한 수준의 보안 및 기밀 보호를 무선랜에 제공하기 위하여 IEEE 802.11 표준에 정의되어 있는 보안 프로토콜로, 무선랜을 통해 전송되는 데이터를 암호화함으로써 유선 네트워크의 물리적인 보안 대책과 동일한 수준의 보안을 제공합니다. WEP를 사용하기 위해서는 무선랜 카드를 연결할 AP 또는 무선 공유기의 보안 설정을 WEP로 하여야 합니다.

- 무선 유틸리티를 이용하여 무선 공유기(또는 AP)에 접속하는 방법입니다.
- 작업 표시줄에 우측에 Rlink 아이콘을 마우스 우측 버튼으로 클릭합니다.
- “Use RaConfig as Configuration utility” 를 클릭하여 Ralink utility를 실행합니다.

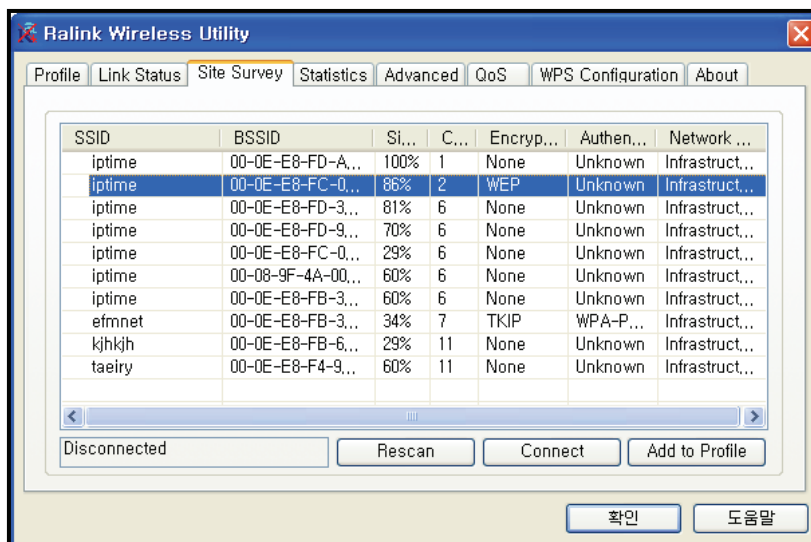


<Ralink 아이콘>



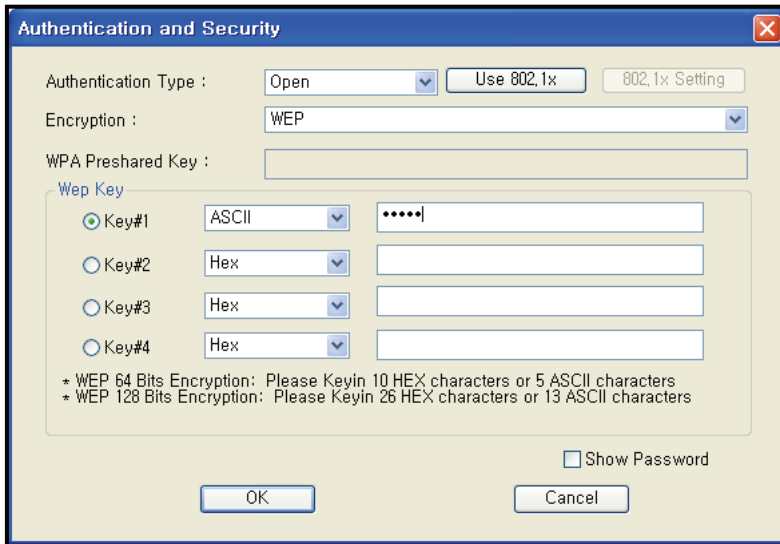
<Ralink utility 실행 하기>

- Site Survey 탭 화면에서 Encrypt가 WEP로 설정된 SSID를 더블 클릭합니다.



<WEP 으로 설정된 SSID 선택 화면>

- 아래와 그림과 같은 화면이 나오면 Network Key에 Key 값을 입력한 후 하단에 있는 OK 버튼을 클릭합니다.



Authentication and Security

Authentication Type : Open Use 802.1x 802.1x Setting

Encryption : WEP

WPA Preshared Key :

Wep Key

☒ Key#1 ASCII

☐ Key#2 Hex

☐ Key#3 Hex

☐ Key#4 Hex

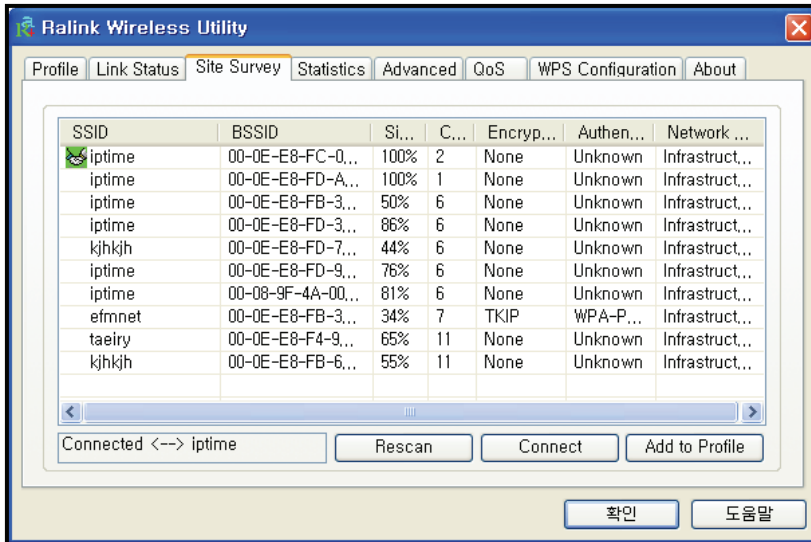
* WEP 64 Bits Encryption: Please Keyin 10 HEX characters or 5 ASCII characters
 * WEP 128 Bits Encryption: Please Keyin 26 HEX characters or 13 ASCII characters

☐ Show Password

OK Cancel

<WEP 설정>

- 선택한 SSID 좌측에 아이콘이 생기면 연결된 것을 확인 할 수 있습니다.



Ralink Wireless Utility

Profile | Link Status | **Site Survey** | Statistics | Advanced | QoS | WPS Configuration | About

SSID	BSSID	Si...	C...	Encryp...	Authen...	Network ...
 iptime	00-0E-E8-FC-0...	100%	2	None	Unknown	Infrastruct...
iptime	00-0E-E8-FD-A...	100%	1	None	Unknown	Infrastruct...
iptime	00-0E-E8-FB-3...	50%	6	None	Unknown	Infrastruct...
iptime	00-0E-E8-FD-3...	86%	6	None	Unknown	Infrastruct...
kjhkjh	00-0E-E8-FD-7...	44%	6	None	Unknown	Infrastruct...
iptime	00-0E-E8-FD-9...	76%	6	None	Unknown	Infrastruct...
iptime	00-08-9F-4A-00...	81%	6	None	Unknown	Infrastruct...
efmnet	00-0E-E8-FB-3...	34%	7	TKIP	WPA-P...	Infrastruct...
taelry	00-0E-E8-F4-9...	65%	11	None	Unknown	Infrastruct...
kjhkjh	00-0E-E8-FB-6...	55%	11	None	Unknown	Infrastruct...

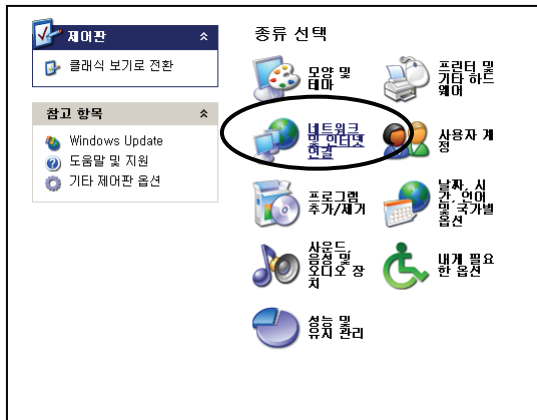
Connected <--> iptime Rescan Connect Add to Profile

확인 도움말

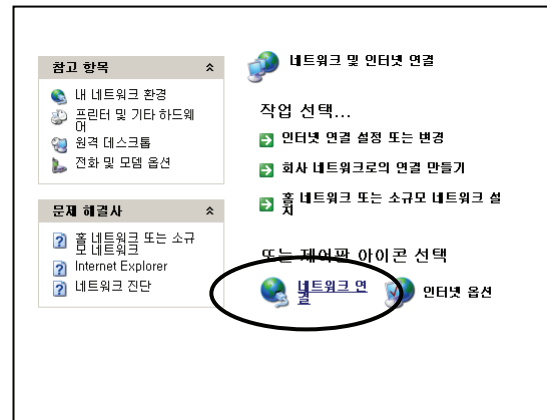
<연결된 SSID>

4.2.3 윈도우 XP에서의 무선 단말 연결

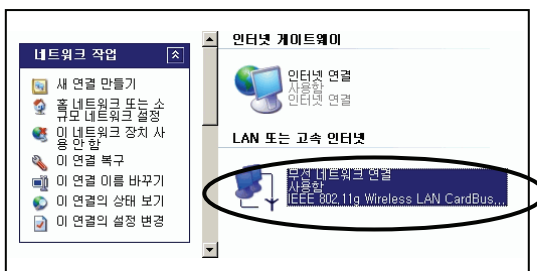
- 윈도우 XP에서는 자체적인 무선 네트워크 관리 유틸리티를 내장하고 있습니다.
- XP내장 무선 유틸리티는 무선랜 카드의 종류에 상관없이 동일한 인터페이스를 제공합니다.
- 무선랜 카드 드라이버 설치과정은 구입하신 랜카드의 설명서를 참고합니다.
- 윈도우 XP 제어판에서 네트워크 및 인터넷 연결을 선택하고 다시 네트워크 연결을 선택합니다.
- 무선 네트워크 연결을 더블 클릭한 후 무선 네트워크 연결 상태 창이 열리면 속성 버튼을 클릭합니다.



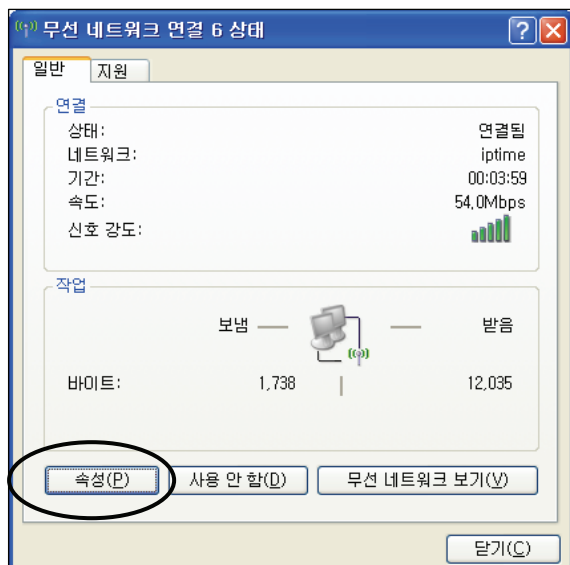
<제어판 화면에서 네트워크연결 선택>



<네트워크 연결 연결 선택>

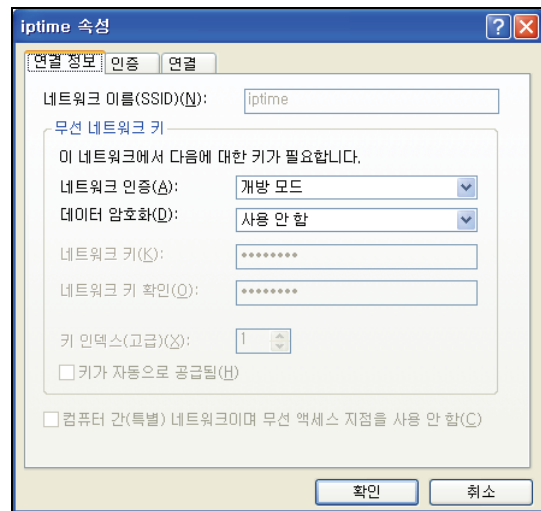
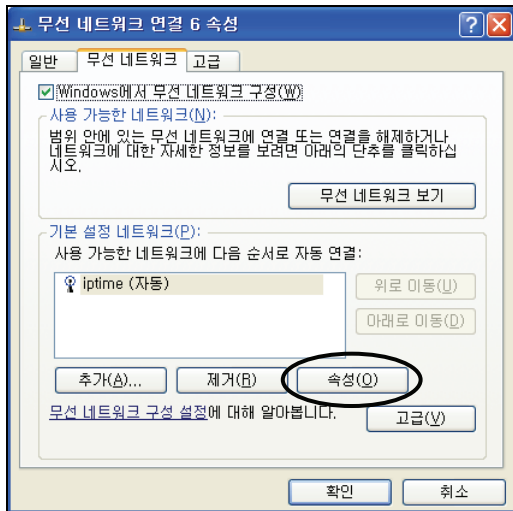


<무선 네트워크 연결 선택>

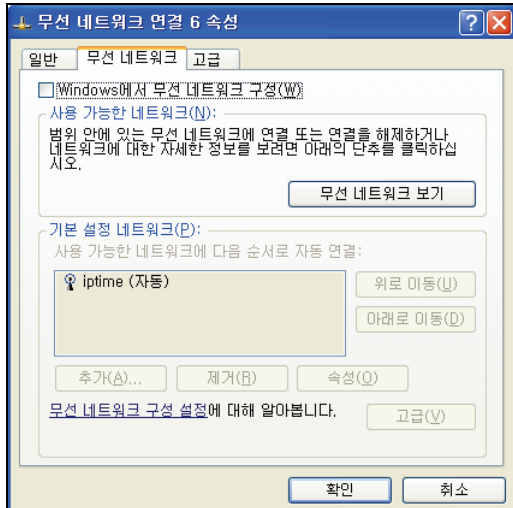


<속성 선택>

- 무선 네트워크 연결 속성 창이 열리면 무선 네트워크 항목을 선택합니다.
- [새로 고침]을 클릭하면 접속 가능한 무선 네트워크의 이름 (SSID)이(가) 표시됩니다.
- 기본 설정네트워크에서 검색되어지 SSID인 iptime외에 다른 아이콘은 제거를 합니다..
- 원하는 네트워크 이름 (SSID)을(를) 선택하고 [속성] 버튼을 클릭하면 해당 네트워크 접속에 필요한 WEP 암호 또는 인증 방식을 선택할 수 있습니다.



- [Windows에서 무선 네트워크 구성]의 Check를 해제하면 98/ME/2000과 같이 무선랜 카드와 같이 제공되는 유틸리티를 이용하여 무선 네트워크를 구성할 수도 있습니다.

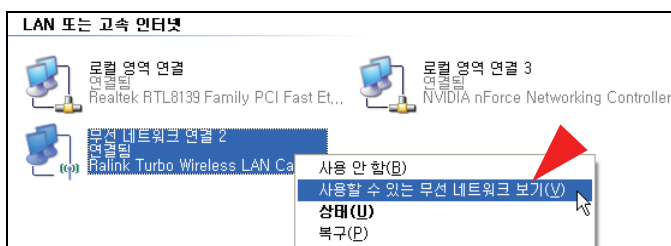


[참고] XP의 무선 네트워크 속성은 운영체제 패치 버전 별로 약간의 구성 화면이 틀릴 수 있습니다.

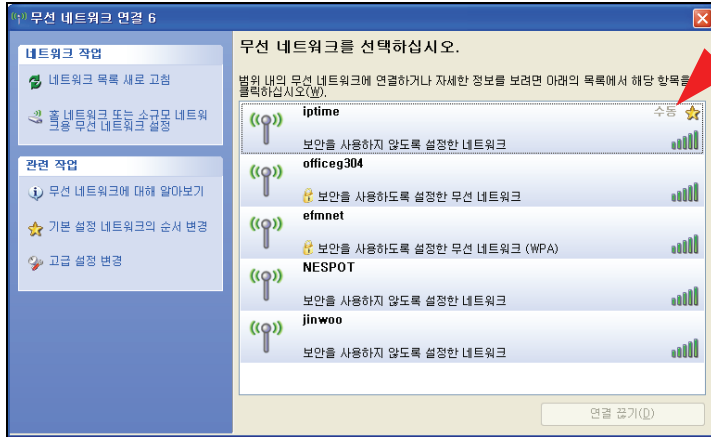
일반적인 무선네트워크연결을 이용한 공유기 SSID 검색 및 연결방법

XP 무선네트워크연결 아이콘을 이용하여 사용할 수 있는 무선네트워크 보기 설정시

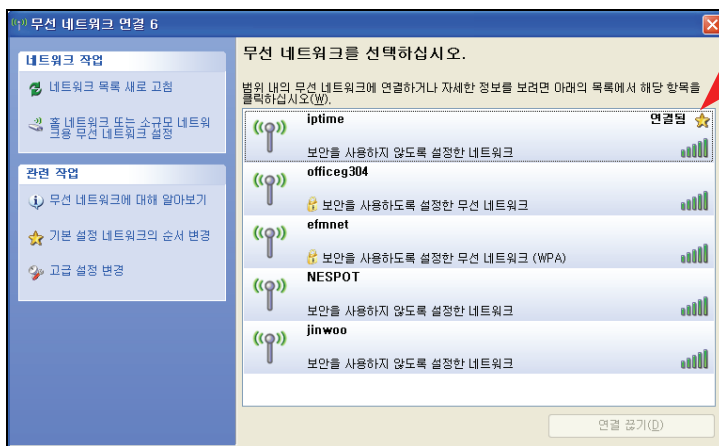
- '무선 네트워크 연결' 을 마우스 오른쪽 버튼을 클릭합니다.
- '사용할 수 있는 무선 네트워크 보기' 를 클릭합니다.



- 공유기에서 설정한 SSID가 검색이 된 경우 “iptime” 을 더블 클릭하면 연결됩니다.



- 정상적인 연결이 될 경우 SSID 오른쪽에 ‘연결됨’ 이라는 메시지가 표시 됩니다.



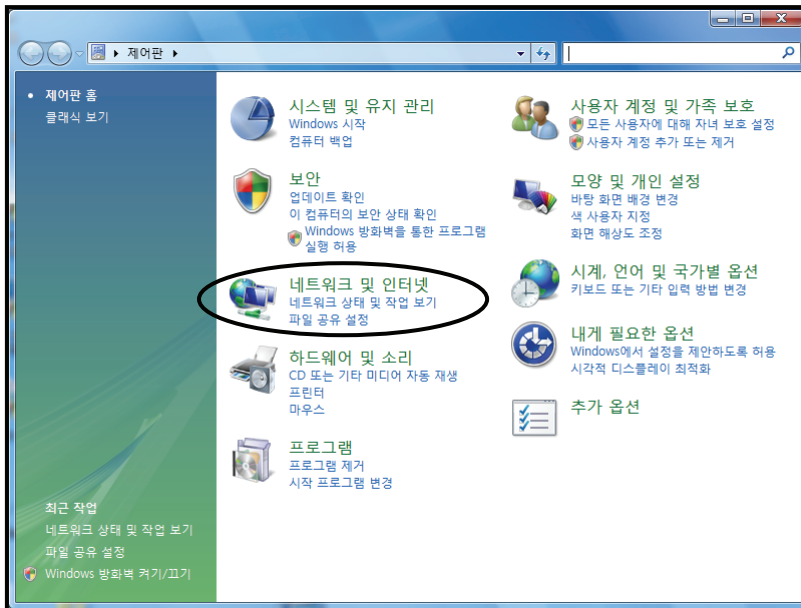
[참고]

유선 랜 연결 후 무선 랜 장착 PC에서 자동으로 인터넷이 연결될 수 있으나 잘못 된 AP 장비로 연결되어 있을 수 있으므로 반드시 무선 연결을 확인하여 고객님의 설정하신 SSID 와 연결이 되어있는지 확인을 하시기 바랍니다.

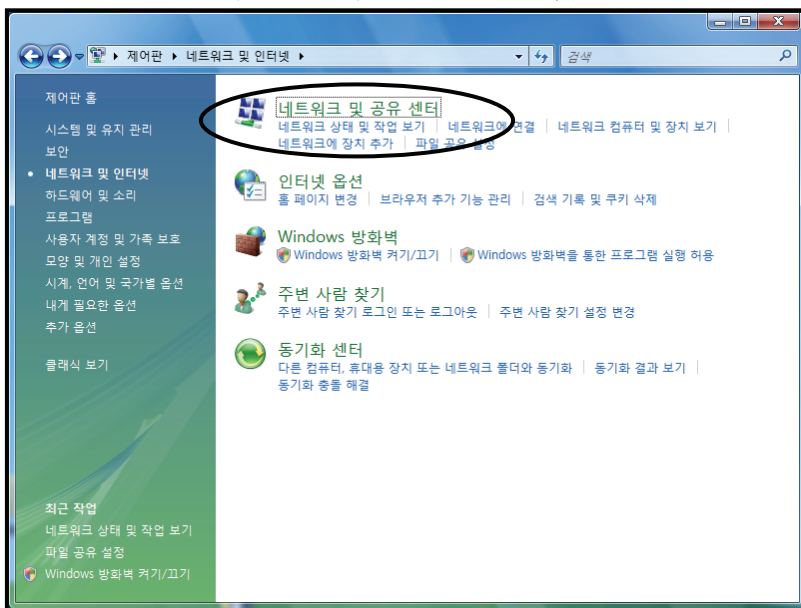


4.2.4 윈도우 VISTA에서의 무선 단말 연결

- 윈도우 VISTA에서는 자체적인 무선 네트워크 관리 유틸리티를 내장하고 있습니다.
- VISTA 내장 무선 유틸리티는 무선 랜카드의 종류에 상관없이 동일한 인터페이스를 제공합니다.
- 무선 랜카드 드라이버 설치 과정은 구입하신 랜카드의 설명서를 참고합니다.
- 제어판에서 네트워크 및 인터넷을 선택하고 다시 네트워크 및 공유센터를 선택합니다.



<제어판에서 네트워크 및 인터넷 선택>



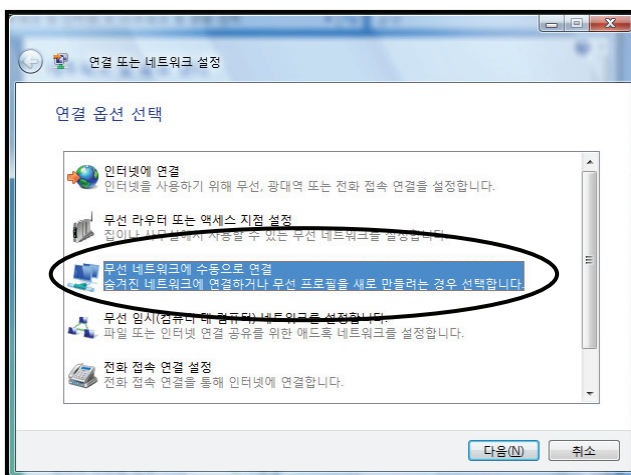
<네트워크 및 공유 센터 선택>

- 아래 그림과 같은 화면이 나오면 연결 또는 네트워크 설정 항목을 선택합니다.



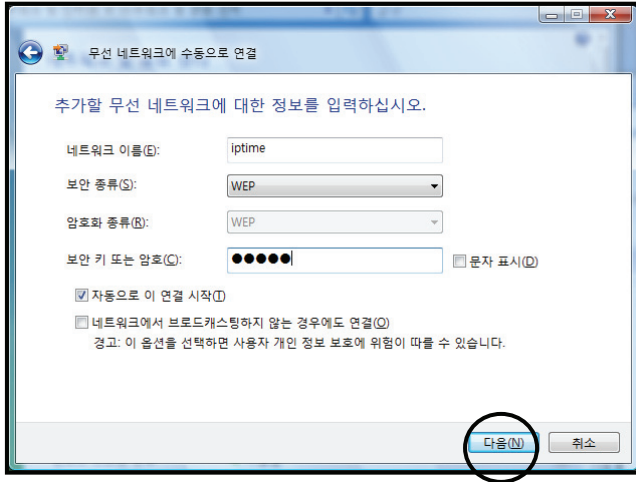
<연결 또는 네트워크 설정 항목 선택>

- 연결 또는 네트워크 설정 창이 열리면 무선 네트워크에 수동으로 연결 항목을 더블 클릭합니다



<무선 네트워크에 수동으로 연결 선택>

- 연결할 네트워크 이름(SSID)을(를) 입력하고 해당 네트워크 접속에 필요한 WEP 암호 또는 인증 방식을 선택, 보안키 또는 암호를 입력하고 다음을 클릭 하면 SSID 추가 확인 창이 보입니다.



무선 네트워크에 수동으로 연결

추가할 무선 네트워크에 대한 정보를 입력하십시오.

네트워크 이름(E):

보안 종류(S):

암호화 종류(B):

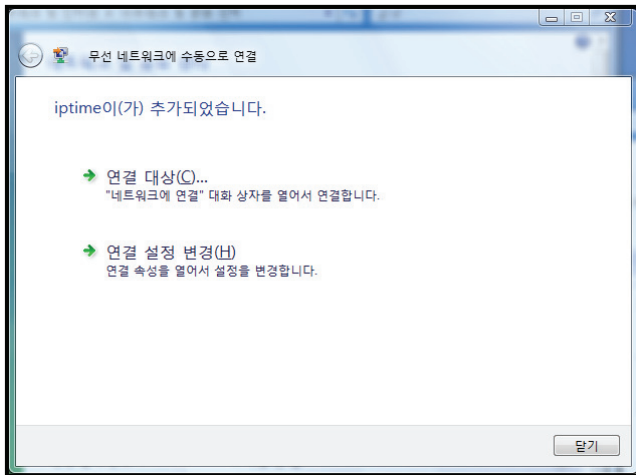
보안 키 또는 암호(C): ☐ 문자 표시(D)

☒ 자동으로 이 연결 시작(O)

☐ 네트워크에서 브로드캐스팅하지 않는 경우에도 연결(O)

경고: 이 옵션을 선택하면 사용자 개인 정보 보호에 위험이 따를 수 있습니다.

<연결 정보 설정>



무선 네트워크에 수동으로 연결

iptime이(가) 추가되었습니다.

→ 연결 대상(C)...
"네트워크에 연결" 대화 상자를 열어서 연결합니다.

→ 연결 설정 변경(H)
연결 속성을 열어서 설정을 변경합니다.

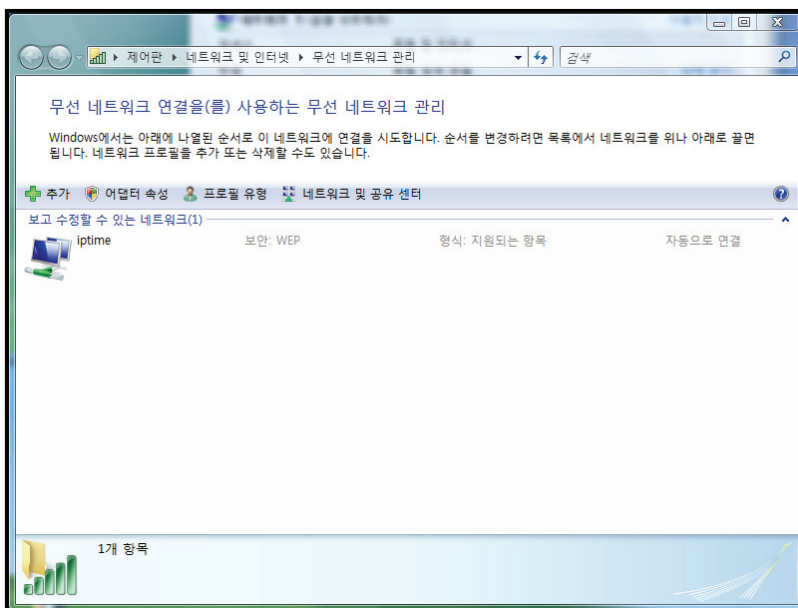
<연결 추가 확인>

- 아래 그림과 같은 화면에서 무선 네트워크 관리를 선택하면 현재 설정된 SSID를 확인할 수 있습니다.



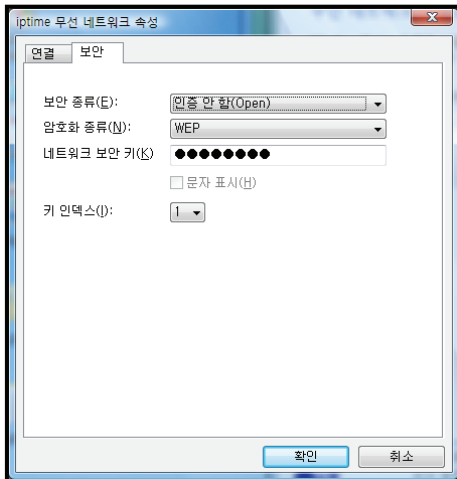
<무선 연결 확인 선택>

- 설정한 SSID인 iptime 외에 다른 아이콘을 제거 합니다. 삭제 하고자 하는 SSID를 선택 후 마우스 오른쪽 버튼을 클릭 후 제거를 선택합니다..



<설정 되어 있는 SSID 목록 화면>

- 설정을 변경하고자 하는 SSID에 마우스 오른쪽 버튼을 클릭 후 속성을 누르고 보안 탭을 선택하면 보안 설정을 변경 할 수 있습니다.



<무선 네트워크 보안 설정 변경>

[참고] VISTA의 무선 네트워크 구성은 무선 랜카드와 같이 제공되는 유틸리티와 동시에 이용 할 수 있습니다.

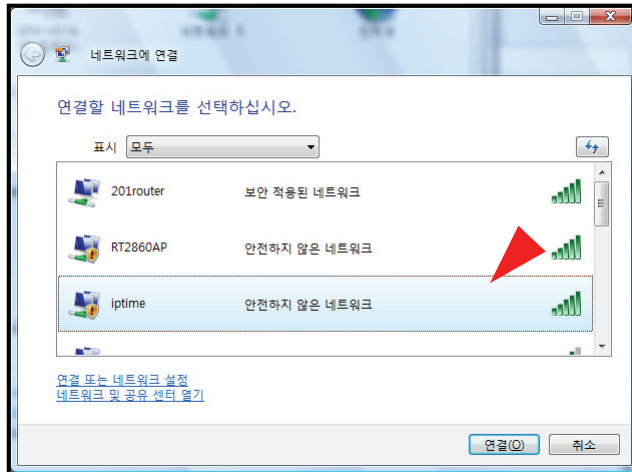
일반적인 무선네트워크연결을 이용한 공유기 SSID 검색 및 연결방법

- 아래 그림과 같은 화면에서 네트워크에 연결을 선택하면 현재 접속 가능한 AP의 목록이 나타납니다.

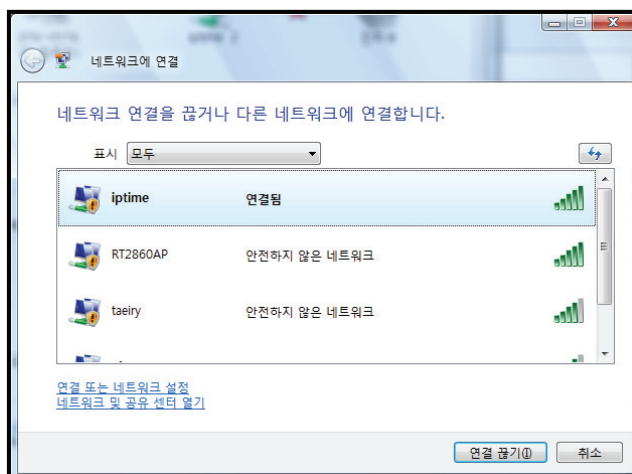


<무선 연결 확인 선택>

- 공유기에서 설정한 SSID가 검색이 된 경우 “iptime” 을 더블 클릭하면 연결됩니다.



- 정상적인 연결이 될 경우 SSID 오른쪽에 ‘연결됨’이라는 메시지가 표시 됩니다.

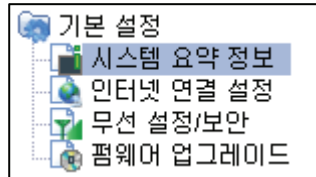


[참고]

유선 랜 연결 후 무선 랜 장착 PC에서 자동으로 인터넷이 연결될 수 있으나 잘못 된 AP 장비로 연결되어 있을 수 있으므로 반드시 무선 연결을 확인하여 고객님의 설정하신 SSID 와 연결이 되어있는지 확인을 하시기 바랍니다.

5장 기본설정

5.1 시스템 요약 정보



공유기의 인터넷 연결 정보, 내부 네트워크 정보, 무선 정보, 펌웨어 정보 그리고 원격 관리 정보를 확인 할 수 있습니다.

인터넷 정보

인터넷 연결 상태	인터넷에 정상적으로 연결됨		
인터넷 연결 방식	고정 IP 연결	외부 IP 주소	210.123.20.245

내부 네트워크 정보

내부 IP 주소	192.168.0.1
DHCP 서버 상태	DHCP 서버 동작중
동적 IP 할당 범위	192.168.0.2 - 192.168.0.254

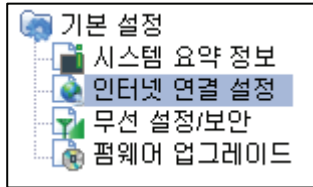
무선 정보

무선 동작 모드	동작중 - AP모드 - 3안테나 MIMO 동작중 - 암호화 사용
SSID(네트워크 이름)	iptime

기타 정보

현재 펌웨어 버전	5.00
원격 관리 정보	원격 관리 포트가 설정되어 있지 않음 [공유기 접속 관리] 에서 설정을 변경 할 수 있습니다.

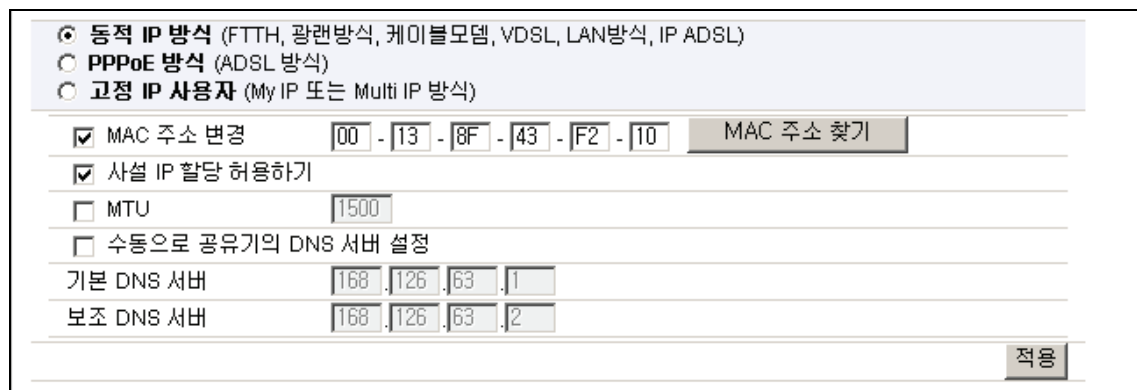
5.2 인터넷 연결 설정



사용하시는 인터넷 서비스 방식을 선택하여 공유기를 인터넷에 연결할 수 있도록 설정하는 메뉴입니다.

5.2.1 동적 IP 방식 설정

FTTH, 광랜, 케이블 모뎀, VDSL, IP-ADSL (접속 프로그램 ADSL 모뎀 내장) 방식의 인터넷 서비스에 접속하는 경우 동적 IP 방식을 선택합니다. 일부 동적 IP 서비스 지역에서는 MAC 주소에 근거하여 서비스를 제한하는 경우가 있습니다. 이때는 모뎀 등에 연결하여 인터넷 사용이 가능한 것으로 확인되는 PC의 MAC 주소를 공유기에 입력해주어야 합니다.



<동적 IP 방식 입력 화면>

동적 IP 방식 설정 항목 요약

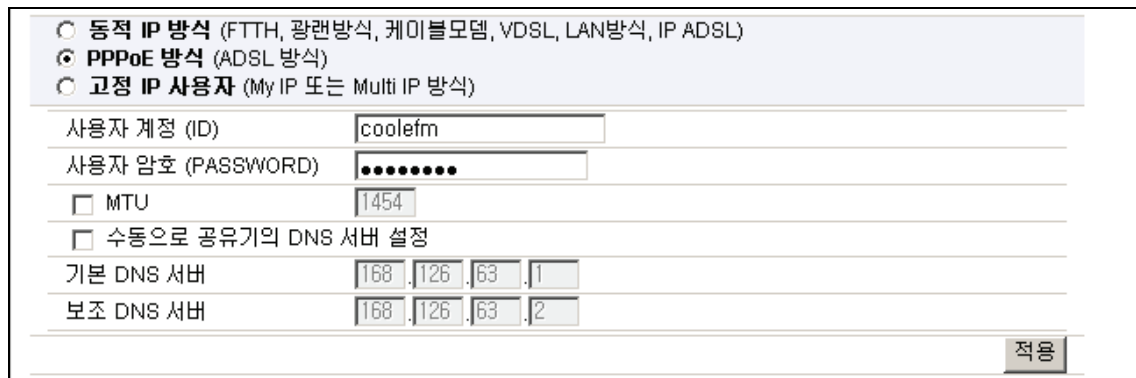
항목	내용
MAC 주소 변경	<u>MAC 주소 변경</u> 에 check를 하면 현재 웹 설정 화면에 접속한 PC의 하드웨어 주소가 자동으로 복사됩니다.
사설 IP 할당 허용하기	WAN 을 사설 IP주소로 구성된 네트워크에 연결하고자 하는 경우 이 항목을 check합니다. 일반적으로 check하지 않고 사용합니다.
MTU	MTU 값은 공유기를 통해서 인터넷으로 전달되는 패킷 데이터의 최대 크기를 지정합니다. 일반적으로 1500을 사용하며 특정한 서비스 환경에서 업로드에 문제가 발생하는 경우 1300정도의 값을 입력하여 사용합니다
수동으로 DNS 서버 설정	인터넷 서비스 회사로부터 자동 할당 받는 DNS 서버를 사용하지 않고 사용자가 지정한 임의의 DNS 서버를 사용할 때 설정합니다.

동적 IP 방식의 WAN 설정 순서

- ① 동적 IP 방식의 ☒ 버튼을 마우스로 클릭하여 선택합니다.
- ② 하드웨어 주소 변경이 필요한 경우에만 입력합니다.
- ③ 하단의 **적용** 버튼을 클릭합니다.
- ④ 인터넷 연결이 확인되면 우측 상단의 **설정저장** 메뉴로 변경 상태를 저장합니다.

5.2.2 PPPoE 방식 설정

Aceman Pro, WinPOET, XP 광대역 접속 프로그램 등을 사용하여 접속하는 ADSL 인터넷 서비스가 PPPoE 방식입니다.



<PPPoE 방식 입력 화면>

PPPoE 방식 설정 항목 요약

항목	내용
사용자 계정	인터넷 서비스 회사에서 전달 받은 사용자 계정
사용자 암호	인터넷 서비스 회사에서 전달 받은 사용자 암호
MTU	PPPoE 통신시 전달되는 Packet의 최대 크기 일반적으로 1454의 값을 사용하며 ADSL 선로 상태가 나빠 끊김이 자주 발생하는 경우 또는 특정 사이트가 접속되지 않는 경우 1300으로 줄여서 사용함.
수동으로 DNS 서버 설정	인터넷 서비스 회사로부터 자동 할당 받는 DNS 서버를 사용하지 않고 사용자가 지정한 임의의 DNS 서버를 사용할 때 설정 합니다.

PPPoE 방식의 WAN 설정 순서

- ① PPPoE 방식의 ☒ 버튼을 마우스로 클릭하여 선택합니다.
- ② 사용자 계정과 암호를 입력합니다.
- ③ 하단의 **적용** 버튼을 클릭합니다.
- ④ 인터넷 연결이 확인되면 우측 상단의 **설정저장** 메뉴로 변경 상태를 저장합니다.

5.2.3 고정 IP 방식 설정

인터넷 회사에서 고정된 IP 주소를 받아서 사용하는 서비스 방식으로 KT의 MY-IP, Multi-IP 등의 서비스가 있습니다.

☐ 동적 IP 방식 (FTTH, 광랜방식, 케이블모뎀, VDSL, LAN방식, IP ADSL) ☐ PPPoE 방식 (ADSL 방식) ☒ 고정 IP 사용자 (My IP 또는 Multi IP 방식)	
외부 IP 주소	210 123 20 245
서브넷 마스크	255 255 255 0
기본 게이트웨이	210 123 20 1
기본 DNS 서버	168 126 63 1
보조 DNS 서버	168 126 63 2
☐ MTU	1500
☒ MAC 주소 변경	00 - 13 - 8F - 43 - F2 - 10 MAC 주소 찾기
적용	

<고정 IP 방식 입력 화면>

고정 IP 방식 설정 항목 요약

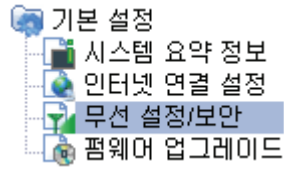
항목	내용
MAC 주소 변경	MAC 주소 변경 에 check를 하면 현재 웹 설정 화면에 접속한 PC의 하드웨어 주소가 자동으로 복사됩니다.
MTU	MTU 값은 공유기를 통해서 인터넷으로 전달되는 패킷 데이터의 최대 크기를 지정합니다. 일반적으로 1500을 사용하며 특정한 서비스 환경에서 업로드에 문제가 발생하는 경우 1300정도의 값을 입력하여 사용합니다

고정 IP 방식의 WAN 설정 순서

- ① 고정 IP 방식의 ☒ 버튼을 마우스로 클릭하여 선택합니다.
- ② 서비스 회사에서 받은 IP주소, 서브넷 마스크, 게이트웨이, DNS 등을 입력합니다.
- ③ 하단의 **적용** 버튼을 클릭합니다.
- ④ 인터넷 연결이 확인되면 우측 상단의 **설정 저장** 메뉴로 변경 상태를 저장합니다.

5.3 무선 설정/보안

무선 AP기능이 제공되는 ipTIME 유무선 공유기 제품에서만 해당되는 내용입니다.



기본 모드는 AP모드이며, 랜카드모드 및 무선WAN 모드 설정을 할 수 있습니다.

* 주의: 랜카드 모드 및 무선 WAN모드를 사용시에는 무선랜 모듈이 랜카드 방식으로 동작하므로, AP기능을 상실합니다.

5.3.1 AP 모드 설정

AP 모드에서는 무선 랜 카드를 가진 PC 나 노트북이 접속하여 인터넷이 가능하게 하며, 가장 일반적인 무선 네트워크의 구성 방법입니다.

동작 설정	☒ 실행 ☐ 중단		
동작 모드	☒ AP 모드 ☐ 랜카드 모드 ☐ 무선 WAN 모드		
네트워크이름(SSID)	ipTIME	모드	g and b
지역	대한민국	채널	ch 6
		최적의 채널 검색	
동작 옵션	SSID(네트워크이름)알림 ☒ 사용함 ☐ 사용하지 않음		
	무선 MAC 주소 복제 ☐ ☐ - ☐ - ☐ - ☐ - ☐ - ☐		
인증방법	자동		
암호화방법	☒ 사용안함 ☐ WEP64 ☐ WEP128 ☐ TKIP ☐ AES		
적용			

AP 모드에서의 설정 항목 요약

항목	기능 설명
동작 설정	무선 AP 기능의 실행/중단 을 결정함
동작 모드	동작 모드를 결정
SSID	무선 네트워크의 이름을 입력함. 사용자가 자유롭게 영문 문자열을 입력함
모드	54Mbps의 g only 모드 또는 11Mbps의 802.11b를 같이 사용할 수 있는 g and b 모드 선택
지역	각국의 전파 규제 법률에 따른 채널 사용 방법 선택
채널	무선 네트워크를 구성하는 채널 선택
최적의 채널검색	최적의 채널을 검색합니다. 채널 검색 시 잠시 무선 연결이 끊길 수 있습니다.
SSID 알림 (동작 옵션 중)	무선 단말기에 SSID를 알려 AP 및 무선 네트워크 존재를 확인함 SSID 알림을 OFF하는 경우 무선 단말기에서 AP가 검색되지 않음
인증/암호화방법	5.3.4 무선보안 을 참고 합니다.

5.3.2 랜카드 모드 설정

랜카드 모드에서는 무선 모듈이 주변의 다른 AP로 접속하여 유무선간 데이터를 브리징 합니다.

랜카드 모드에서는 최초 인식된 유선 PC한대만 무선으로 브리징 됩니다.

이 기능은 무선 랜 카드를 장착하기 힘든 게임기 또는 PC에서 유선랜을 무선랜으로 확장하고자 할 경우에 사용됩니다.

* 랜카드모드를 사용하면 무선AP로서의 기능이 동작하지 않습니다.

동작 설정	☒ 실행 ☐ 중단		
동작 모드	☐ AP 모드 ☒ 랜카드 모드 ☐ 무선 WAN 모드		
네트워크이름(SSID)	iptime	연결할 AP검색	모드 g and b
지 역	대한민국	채널	ch 6
동작 옵션	SSID(네트워크이름)알림 ☒ 사용할 ☐ 사용하지 않음		
인증방법	무선 MAC 주소 복제 ☐ ☐ - ☐ - ☐ - ☐ - ☐ - ☐		
암호화방법	자동		
	☒ 사용안함 ☐ WEP64 ☐ WEP128 ☐ TKIP ☐ AES		
적용			

랜카드 모드에서의 설정 항목 요약

항목	기능 설명
동작 설정	무선 랜카드 기능의 실행/중단 을 결정함
동작 모드	동작 모드를 결정
SSID	연결할 무선 네트워크의 이름을 입력함.
연결할 AP검색	주변의 무선네트워크를 검색하여, 연결할 AP를 찾음.
모드	54Mbps의 g only 모드 또는 11Mbps의 802.11b를 같이 사용할 수 있는 g and b 모드 선택
지역	각국의 전파 규제 법률에 따른 채널 사용 방법 선택
채널	랜카드 모드에서는 연결될 AP의 채널로 자동으로 설정됨.
무선 MAC주소복제	무선 모듈의 MAC주소를 변경합니다.
인증/암호화방법	5.3.4 무선보안 을 참고 합니다.

5.3.3 무선 WAN 모드 설정

무선 WAN 모드에서는 무선 모듈이 주변의 다른 AP로 접속한 후, WAN포트의 기능을 수행합니다. 이 모드를 사용할 경우에는 유선WAN포트를 사용하지 않게 되므로, 일반적인 인터넷 서비스 방식에서는 사용될 수 없습니다.

* 무선 WAN모드를 사용하면 무선AP로서의 기능이 동작하지 않습니다.

동작 설정	☒ 실행 ☐ 중단		
동작 모드	☐ AP 모드 ☐ 랜카드 모드 ☒ 무선 WAN 모드		
네트워크이름(SSID)	ipTIME	연결할 AP검색	모드 g and b ▼
지 역	대한민국 ▼		채널 ch 6 ▼
동작 옵션	SSID(네트워크이름)알림 ☒ 사용함 ☐ 사용하지 않음		
	무선 MAC 주소 복제 ☐ ☐ - ☐ - ☐ - ☐ - ☐ - ☐		
인증방법	자동 ▼		
암호화방법	☒ 사용안함 ☐ WEP64 ☐ WEP128 ☐ TKIP ☐ AES		
적용			

무선 WAN모드에서의 설정 항목 요약

항목	기능 설명
동작 설정	무선 랜카드 기능의 실행/중단 을 결정함
동작 모드	동작 모드를 결정
SSID	연결할 무선 네트워크의 이름을 입력함.
연결할 AP검색	주변의 무선네트워크를 검색하여, 연결할 AP를 찾음.
모드	54Mbps의 g only 모드 또는 11Mbps의 802.11b를 같이 사용할 수 있는 g and b 모드 선택
지역	각국의 전파 규제 법률에 따른 채널 사용 방법 선택
채널	연결될 AP의 채널로 자동으로 설정됨.
인증/암호화방법	5.3.4 무선보안 을 참고 합니다.

5.3.4 무선 보안

무선 보안 기능을 사용하면 무선 네트워크를 보안 안전하게 외부의 침입으로부터 보호할 수 있습니다.

무선 보안을 설정하려면 아래의 3단계의 과정을 거쳐야 합니다.

1) 인증방법 선택

인증방법	자동	
암호화방법	자동 개방 모드 공유 모드 WPAPSK WPA2PSK WPAPSK/WPA2PSK	64 ☐ WEP128 ☐ TKIP ☐ AES
		적용

인증 방법	기능 설명
자동	개방/공유모드를 자동으로 선택합니다.(기본값)
개방 모드	모든 사용자에게 인증을 허용합니다.
공유 모드	정확한 네트워크 키를 가진 사용자에게 인증을 허용합니다.
WPAPSK	공유모드에서 보안이 강화된 WPA인증 표준입니다.
WPA2PSK	보다 향상된 WPA인증 표준입니다.
WPAPSK/WPA2PSK	WPAPSK와 WPA2PSK를 동시에 지원합니다.

2) 암호화 방법 선택

아래의 5개의 암호화 방법중 한가지를 선택합니다.

해당 인증방법에 맞는 암호화 방법만 선택이 가능합니다.

암호화 방법	인증방법	기능 설명
사용안함	자동모드	암호화를 사용하지 안함.
	개방모드	(인증 방법이 자동 또는 개방 모드일 경우에만 가능)
WEP64	자동모드	64Bit 키를 사용하여 WEP암호화 방법 사용
WEP128	공유모드	128Bit 키를 사용하여 WEP암호화 방법 사용
TKIP	WPAPSK	WEP보단 보안을 강화한 암호화 방법
AES	WPA2PSK	보안을 강화한 새로운 암호화 방법

3) 네트워크 키 입력

WEP64 또는 WEP128 선택시 네트워크 키 입력 예

암호화방법	☐ 사용안함 ☒ WEP64 ☐ WEP128 ☐ TKIP ☐ AES			
네트워크 키	KEY 입력 방법	☒ 문자열 ☐ 16진수		
	기본 KEY 선택	☒ 1 ☐ 2 ☐ 3 ☐ 4		
	Key 값을 입력하십시오	1:	12345	
		2:		
3:				
4:				
적용				

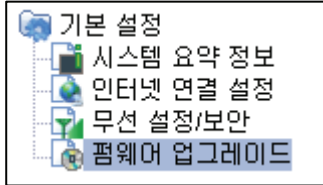
- KEY 입력방법은 일반적으로 문자열을 선택합니다.
- 기본 KEY를 1,2,3,4 중 선택합니다.
- 키 값은 1,2,3,4중 한 개 이상을 채워서 입력해야 합니다.
- 입력된 키는 무선 단말에서 접속 시 필요합니다.

TKIP/AES 선택시 네트워크 키 입력 예

암호화방법	☐ 사용안함 ☐ WEP64 ☐ WEP128 ☒ TKIP ☐ AES
네트워크 키	

- 네트워크 키 값을 8글자 이상 입력합니다.
- 입력된 키는 무선 단말에서 접속 시 필요합니다.

5.4 펌웨어 업그레이드



새로 배포되는 ipTIME 펌웨어를 해당 메뉴에서 업그레이드 할 수 있다.

자동 업그레이드

공유기가 인터넷에 정상적으로 연결된 경우에는 **자동 업그레이드 실행하기**를 클릭하고 해당 프로그램 열기를 선택하면 아래 그림과 같은 펌웨어 업그레이드 유틸리티가 실행되고 공유기의 최신 펌웨어로 자동 업그레이드 됩니다.

펌웨어 업그레이드

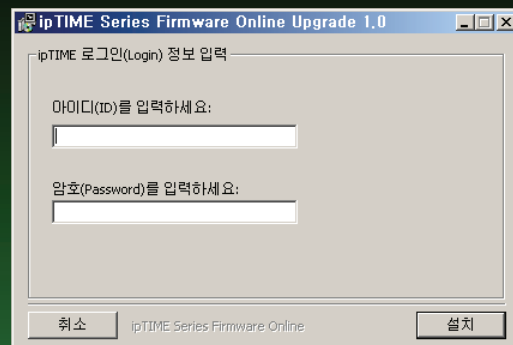
현재 펌웨어 버전	5.00
만든 날짜	Fri Apr 13 18:16:19 KST 2007

☒ 자동 업그레이드 ☐ 수동 업그레이드

자동 업그레이드를 실행하면 [ipTIME 홈페이지]에 배포된 펌웨어의 최신버전을 확인하여, 공유기의 펌웨어를 최신버전으로 업그레이드 합니다.
 1. [자동 업그레이드 실행하기] 버튼을 클릭합니다.
 2. 팝업창이 뜨면 [실행] 버튼을 눌러 프로그램(upgrade.exe)을 실행합니다.

자동 업그레이드 실행하기

ipTIME Series Firmware Online Upgrade 1.0



ipTIME Series Firmware Online Upgrade 1.0

ipTIME 로그인(Login) 정보 입력

아이디(ID)를 입력하세요:

암호(Password)를 입력하세요:

취소 ipTIME Series Firmware Online 설치

수동 업그레이드

수동 업그레이드를 위해 <http://www.iptime.co.kr>을 방문하여 **고객지원** >> **네트워크** >> **다운로드** >> **펌웨어 수동 업데이트**를 클릭하여 제품 모델명을 선택한 후 해당 제품의 최신 펌웨어를 PC에 저장합니다.

[참고] 파일 1 : 한글 버전 펌웨어 파일 2 : 영문 버전 펌웨어


펌웨어 자동 업데이트


펌웨어 수동 업데이트


제품 설명서 다운로드


유틸리티 다운로드

제품 모델명
선택 하세요 ▼

번호	제목	날짜	조회
13	ipTIME G304 펌웨어 버전 2.40	2007/03/16	3563
12	ipTIME G304 펌웨어 버전 2.32	2007/03/10	1723
11	ipTIME G304 펌웨어 버전 2.30	2007/03/08	879
10	ipTIME G304 펌웨어 버전 2.28	2007/02/27	1698
9	ipTIME G304 펌웨어 버전 2.26	2007/01/23	3767
8	ipTIME G304 펌웨어 버전 2.24	2006/11/07	5234
7	ipTIME G304 펌웨어 버전 2.22 (베타)	2006/10/25	1212
6	ipTIME G304 펌웨어 버전 2.18	2006/09/14	2989
5	ipTIME G304 펌웨어 버전 2.08	2006/07/04	3238
4	ipTIME G304 펌웨어 버전 2.04	2006/06/13	1257
3	ipTIME G304 펌웨어 버전 2.00	2006/05/24	840
2	ipTIME G304 펌웨어 버전 1.98	2006/05/15	594
1	ipTIME G304 펌웨어 버전 1.94 (베타)	2006/04/26	741

<ipTIME 홈페이지 펌웨어 다운로드, 홈페이지는 당사 사정에 따라 변동될 수 있음>

펌웨어 업그레이드

현재 펌웨어 버전	5.00
만든 날짜	Fri Apr 13 18:16:19 KST 2007

☐ 자동 업그레이드
☒ 수동 업그레이드

수동 업그레이드를 통해 공유기의 펌웨어를 업그레이드할 수 있습니다.

1. [ipTIME홈페이지]에서 펌웨어를 다운로드합니다.
2. [찾아보기] 버튼을 누른 후, 다운로드받은 펌웨어파일을 선택합니다.
3. [업그레이드] 버튼을 클릭합니다.

찾아보기...

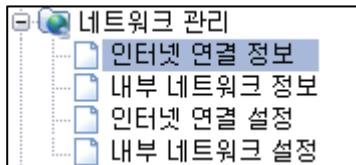
업그레이드

공유기 설정 화면에서 **찾아보기** 버튼을 클릭하여 다운 받은 펌웨어를 선택합니다.

업그레이드 버튼을 클릭하여 최신 버전의 펌웨어로 업그레이드를 시작합니다.

6장 네트워크 관리

6.1 인터넷 연결 정보



ipTIME의 인터넷 연결 상태 확인 할 수 있습니다.

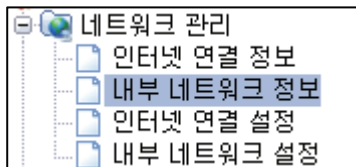
인터넷 회선 상태를 반영하기 위하여 연결이 되지 않은 경우 5초마다 자동 갱신됩니다.

연결 상태	인터넷에 정상적으로 연결됨
연결 방식	PPPoE 연결
외부 IP 주소	61.77.128.248
서브넷 마스크	255.255.255.255
기본 게이트웨이	61.77.128.248
기본 DNS 서버	168.126.63.1
보조 DNS 서버	168.126.63.2
MAC 주소	00-08-9F-29-71-D2

[접속 해제](#)

■ 위의 예는 PPPoE 방식의 인터넷 연결 정보입니다.

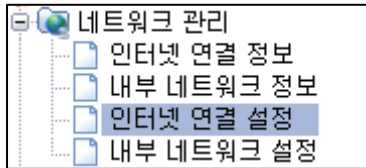
6.2 내부 네트워크 정보



ipTIME의 내부 네트워크 설정 정보, 내장된 DHCP서버가 할당한 동적 IP 할당 수 및 ipTIME과 연결되어 있는 PC들의 정보를 확인할 수 있습니다.

내부 네트워크 정보			
내부 IP 주소	192.168.0.1		
서브넷 마스크	255.255.255.0		
MAC 주소	00-08-9F-28-71-D2		
동적 IP 할당 범위	192.168.0.2 ~ 192.168.0.254		
동적 IP 할당 수	3		
사용 중인 IP 주소 정보			
	IP 주소	MAC 주소	비고
1	192.168.0.210	00-08-9F-28-1A-28	유선 : 수동설정
2	192.168.0.11	00-13-8F-43-F2-10	유선 : 수동설정

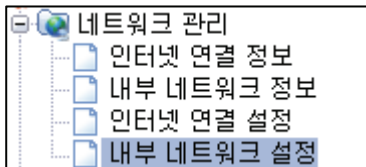
6.3 인터넷 연결 설정



사용하시는 인터넷 서비스 방식을 선택하여 공유기를 인터넷에 연결할 수 있도록 설정하는 메뉴입니다.

자세한 내용은 5.2절 기본설정의 인터넷 연결 설정을 참고하세요.

6.4 내부 네트워크 설정



ipTIME의 내부 IP 설정, DHCP 서버의 설정 및 DHCP 서버의 수동 IP 할당 설정을 할 수 있습니다.

내부 IP 설정

ipTIME의 기본 IP 주소는 192.168.0.1입니다. 이 IP 주소를 변경하고자 하는 경우 본 항목을 이용합니다

내부 IP 설정				
내부 IP 주소	192	168	0	119
서브넷 마스크	255	255	255	0
적용 후 시스템 재시작				

적용 후 시스템 재시작 버튼을 클릭하면 공유기의 IP 주소가 변경되며 아래 화면과 같이 변경 IP 주소 적용을 위한 공유기 재시작 화면이 표시된 후 내부 IP 주소가 변경됩니다.

내부IP가 변경되어, 공유기가 재시작되고 있습니다.
진행상태가 완료되면 자동으로 현재 페이지로 접속됩니다.
잠시만 기다리십시오.

[참고] 내부 IP 주소 변경은 별도 설정저장 없이도 자동으로 저장됩니다

DHCP 서버 상태/설정

DHCP 서버 설정에서 실행 또는 중지를 선택한 후 적용 버튼을 클릭하여 ipTIME의 DHCP 서버를 켜거나 끌 수 있습니다. DHCP 서버를 중지하면 ipTIME에서 PC로 IP주소를 자동 할당하지 않습니다.

DHCP 서버 상태/설정

DHCP 서버 설정

☒ 실행
 ☐ 중지

DNS Suffix

local

동적 IP주소 범위

192

.168

.0

.1

~

192

.168

.0

.254

☐ 내부네트워크에서 DHCP서버 발견시 공유기의 DHCP 서버기능을 중단
☐ IP를 할당받은 PC만 인터넷 접속을 허용

적용

무선 접속 정보화면에서 표시되는 내용은 다음과 같습니다.

동작 상태	무선 모듈의 동작상태
DHCP 서버 설정	DHCP 서버의 동작을 설정합니다.
DNS Suffix	DNS suffix를 정의하면 자동으로 클라이언트 이름 뒤에 도메인 이름이 붙게 됩니다 예를 들어, DNS suffix를 'office.com'으로 지정한 후, 'abc' 라는 클라이언트 이름으로 ping 테스트를 하게 되면 "abc.office.com" 도메인 이름에 대한 DNS 쿼리가 송신됩니다
동적 IP 주소 범위	DHCP 서버가 PC에 자동 할당해 줄 수 있는 IP 주소의 범위를 설정 할 수 있습니다. 예를 들어, '192.168.0.[10] ~ 192.168.0.[100]'으로 설정하면, PC들은 192.168.0.10부터 IP 주소를 자동할당 받게 됩니다

정상적인 IP 주소 할당을 위해서는 DHCP 서버를 실행하여야 하며 DHCP 서버를 중단 시킨 경우라면 ipTIME에 연결하는 PC의 IP 주소는 수동으로 설정하여 사용하여야 합니다.

IP 주소 수동 설정 방법은 본사 홈페이지(<http://www.iptime.co.kr>)에서 고객지원 >> 네트워크 >> 자주묻는질문 게시판에서 확인하시기 바랍니다

내부네트워크에서 DHCP 서버 발견시 공유기의 DHCP 서버기능을 중단합니다.

ipTIME 내부 네트워크에 다른 DHCP 서버가 발견되면 공유기는 DHCP 기능을 중단하게 되며, DHCP가 다시 발견되지 않으면 자동으로 DHCP 기능을 실행하게 됩니다.

DHCP 서버에서 IP를 할당받은 PC만 인터넷 접속을 허용합니다.

ipTIME에 연결된 PC 랜카드의 TCP/IP 설정이 자동으로 IP 주소 받기로 설정되어 있는 PC만 인터넷 접속을 허용하는 기능입니다. TCP/IP 설정이 수동으로 구성되어 있는 경우 인터넷 접속이 차단됩니다.

수동 IP 할당 설정

DHCP 서버가 특정PC에게 설정해 놓은 IP로만 할당 하게 합니다.

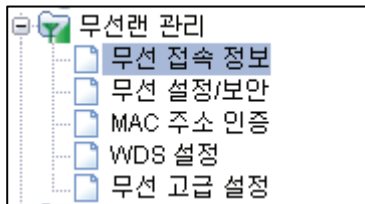
수동 IP 할당 설정											
삭제 <table border="1"> <thead> <tr> <th></th> <th>☐ 설정된 IP/MAC주소</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>☐ 192.168.0.47 / 00-08-9F-28-7D-C8</td> </tr> <tr> <td>2</td> <td>☐ 192.168.0.57 / 00-63-00-00-04-74</td> </tr> <tr> <td>3</td> <td>☐ 192.168.0.210 / 00-08-9F-28-1A-28</td> </tr> </tbody> </table>		☐ 설정된 IP/MAC주소	1	☐ 192.168.0.47 / 00-08-9F-28-7D-C8	2	☐ 192.168.0.57 / 00-63-00-00-04-74	3	☐ 192.168.0.210 / 00-08-9F-28-1A-28	추가 <table border="1"> <thead> <tr> <th>☐ 검색된 IP/MAC주소</th> </tr> </thead> <tbody> <tr> <td> ☐ 192.168.0. / - - - - - ☐ 192.168.0.208 / 00-17-31-F4-37-8D 현재 접속된 PC </td> </tr> </tbody> </table>	☐ 검색된 IP/MAC주소	☐ 192.168.0. / - - - - - ☐ 192.168.0.208 / 00-17-31-F4-37-8D 현재 접속된 PC
	☐ 설정된 IP/MAC주소										
1	☐ 192.168.0.47 / 00-08-9F-28-7D-C8										
2	☐ 192.168.0.57 / 00-63-00-00-04-74										
3	☐ 192.168.0.210 / 00-08-9F-28-1A-28										
☐ 검색된 IP/MAC주소											
☐ 192.168.0. / - - - - - ☐ 192.168.0.208 / 00-17-31-F4-37-8D 현재 접속된 PC											

- 검색된 IP/MAC주소를 추가
 - 추가할 IP/MAC주소 좌측의 체크박스를 클릭
 - 추가 버튼 클릭
- 검색되지 않은 IP/MAC주소를 등록
 - 첫번째 줄의 체크박스를 클릭한 후, IP/MAC주소를 입력
 - 추가 버튼 클릭
- 설정된 IP/MAC주소를 삭제
 - 삭제할 IP/MAC주소 좌측의 체크박스 클릭
 - 삭제 버튼 클릭

7장 무선랜 관리

7장은 무선 AP기능이 제공되는 ipTIME 유무선 공유기 제품에서만 해당되는 내용입니다.

7.1 무선 접속 정보



무선 동작 상태에 관련된 정보인 SSID, 모드, 채널, SSID 알림 기능 여부, 인증방법, 암호화 방법, MAC 주소 인증 여부 등을 확인할 수 있습니다.

무선 설정 상태				
동작 상태	동작중 - AP모드			
SSID(네트워크 이름)	iptime			
모드	G and B			
지 역	대한민국			
채널	6			
SSID(네트워크이름) 알림 기능	동작중			
인증방법	자동인증			
암호화방법	암호화 사용안함			
MAC 주소 인증	모두 허용			
무선 MAC 주소	00-0E-E8-56-80-FF			

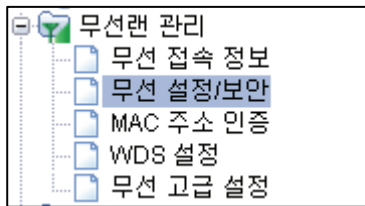
무선 클라이언트 정보				
				통계 초기화
MAC 주소	연결상태	수신패킷	송신패킷	마지막 통신시각
1 00-19-D2-89-D2-8A	54 Mbps	105908	293282	2007-04-17 19:59:28

무선 접속 정보화면에서 표시되는 내용은 다음과 같습니다.

동작 상태	무선 모듈의 동작상태
동작 상태	무선 동작 모드 및 상태
SSID(네트워크 이름)	무선 랜에서 무선 검색 시 검색되어 지는 네트워크 이름
모드	G only : 802.11G(54Mbps)기반의 호스트만 접속. G and B : 802.11G(54Mbps)와 802.11B(11Mbps)기반 접속
지 역	전파 송신 지역
채널	채널은 대한민국 에서 1-13번 중 선택가능
SSID(네트워크이름) 알림	SSID를 모든 무선 호스트에 알려주는 기능
인증 방법	무선 호스트가 공유기에 인증하는 방법
암호화 방법	무선호스트가 공유기와 통신하는 데이터의 암호화 방법
MAC 주소 인증	MAC주소를 통한 인증방법
무선 MAC 주소	무선 AP의 하드웨어 주소

- 무선 클라이언트 정보 - 현재 ipTIME에 접속되어 있는 무선 클라이언트의 정보를 보여 줍니다.

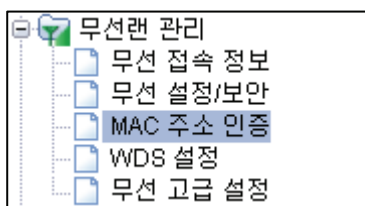
7.2 무선 설정/보안



무선 관련 설정 메뉴입니다.

자세한 내용은 5.3절 기본설정의 무선설정/보안을 참고하세요.

7.3 MAC 주소 인증



MAC 주소 인증 기능을 이용하여 등록된 MAC 주소에 대해서 세 가지의 정책을 적용할 수 있습니다. 적용할 수 있는 정책은 `모두허용`, `등록된 주소만 허용`, `등록된 주소만 차단`이 있습니다.

☒ 모두 허용
 ☐ 등록된 주소만 허용
 ☐ 등록된 주소만 차단

적용

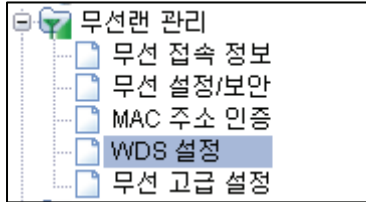
삭제	등록된 무선 MAC 주소
1	☐ 00-0E-E8-FC-00-8A
2	☐ 00-0E-E8-FB-39-98
3	☐ 00-18-39-2C-3A-DE
4	☐ 00-0E-E8-52-0D-09

추가	검색된 무선 MAC 주소
☐	- - - - -
☐	00-0E-E8-FD-8D-14
☐	00-08-9F-FE-17-1B
☐	00-0E-E8-F4-76-BF
☐	00-0E-2E-89-19-B0
☐	00-0C-F1-37-A5-06
☐	00-08-9F-FF-47-F1
☐	00-11-F5-DB-0B-00
☐	00-08-9F-FE-1A-3C
☐	00-16-6F-35-00-96
☐	00-08-9F-FE-C8-5F
☐	00-13-10-DB-22-C0
☐	00-0E-E8-FD-33-02

등록 가능한 최대 MAC 주소는 50개 입니다.

- 일반적인 경우 `등록된 주소만 허용`을 선택하면 편리하며 검색된 주소를 추가하여 사용합니다.
- 검색된 주소를 추가하는 경우 검색된 주소를 check하고 추가 버튼을 클릭합니다.
- 무선 단말의 MAC 주소를 알고 계신 경우 수동입력에서 주소 값을 입력 후 추가 버튼을 클릭합니다.

7.4 WDS 설정



WDS (무선 유통 시스템)을 통해 ipTIME은 무선으로 다른 WDS가 지원되는 Access Points와 연결되고, 여러 개의 Access Points가 반복될 수 있습니다.

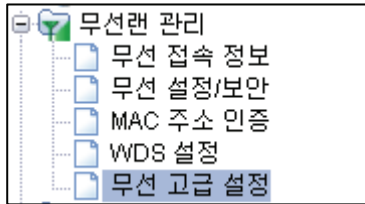
- point-to-point 및 point-to-multipoint bridging 기능을 지원
- ipTIME의 경우는 10 Point까지 지원됨

연결할 AP의 무선 MAC 주소(BSSID)	설명
- - - - - 연결할 AP검색	
등록 가능한 최대 AP의 개수는 4개 입니다. 추가	
연결할 AP의 무선 MAC 주소(BSSID)	설명
1 00-0E-E8-FD-8D-12	iptime_wds
	삭제

WDS 설정에 필요한 각각의 항목은 다음과 같습니다.

설정 항목	기능 설명
연결할 AP의 무선MAC주소	WDS로 연결할 대상 AP의 MAC 주소를 입력합니다
설명	연결을 구분할 설명을 입력합니다.
추가	버튼을 클릭하여 입력한 상대 AP 정보를 추가 합니다

7.5 무선 고급 설정

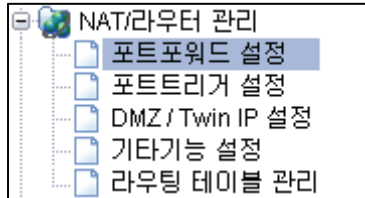


무선 고급 설정은 무선 네트워크에 익숙한 고급사용자를 위한 설정입니다.

송신 파워	송신 파워를 조절하여 무선 전파가 전달되는 범위를 조절할 수 있습니다. 설정 값이 높을수록 무선 전파 전달 범위가 넓어집니다.
Tx Burst	이 기능 사용시 무선의 최대 속도를 올릴 수 있습니다. 그러나, 동시에 연결되는 무선Station의 수가 많을 경우에는, 안정적인 무선 통신을 위하여 이 기능을 끄기를 권장합니다
Frame Aggregation	이 기능을 지원하는 ipTIME G054P, G300P, G054U2등의 무선 랜카드와 함께 사용할 경우 무선의 성능을 비약적으로 올릴 수 있습니다
Short Slot	이 기능을 사용하면 11g로 연결된 무선Station의 성능을 향상시킬 수 있습니다. 하지만, 무선통신이 원활하지 않은 무선Station이 존재한다면, 이 기능을 끄고 시도하기를 권장합니다.
Preamble 길이	Short Preamble로 설정할 경우에는 약간의 성능 향상을 기대할 수 있습니다. 그러나 초기 무선 랜카드 제품등과 연결시 호환성이 떨어질 수 있습니다. 최고의 호환성을 위해서는 Long Preamble을 사용하는 것이 좋습니다.
RTS Threshold	설정 값 이상의 길이를 가진 무선 데이터 전송시 RTS/CTS방식으로 데이터를 전송합니다. 이 값을 작게 할수록 더욱 안정적인 무선통신을 보장하지만, 최대 속도는 감소합니다. 동시에 연결되는 무선 Station의 수가 많을 수록 작은 값을 사용하는 것이 좋습니다. 설정 가능한 값은 1 ~ 2347 입니다.
Fragmentation Threshold	설정 값 이상의 길이를 가진 무선 데이터 전송시 설정값 크기로 데이터를 나누어 전송합니다. 이 값을 작게 할수록 더욱 안정적인 무선 통신을 보장하지만, 최대 속도는 감소합니다. 주변의 다른 신호에 의한 간섭이 많을 경우에 작은 값을 사용하는 것이 좋습니다. 설정 가능한 값은 256 ~ 2346 입니다.
BG Protection	11b와 11g 용 랜카드를 동시에 사용하는 경우 원활한 무선 통신을 위한 설정입니다. 일반적으로 자동 설정을 권장합니다.
Beacon 주기	Beacon이 전송되는 주기를 조절할 수 있습니다. 일반적으로 100ms를 사용합니다. 설정할 수 있는 값의 범위는 50 ~ 1024 입니다.

8장 NAT/라우터 관리

8.1 포트포워드 설정



공유기의 외부 네트워크 사용자가 내부 네트워크에 접속하고자 하는 경우 사용되는 어플리케이션의 포트번호를 내부 네트워크의 IP 주소와 내부포트 번호로 연결시켜주는 기능이 필요한데, 이런 기능을 포트포워드라고 합니다.

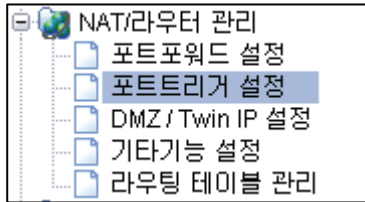
정의된 리스트	사용자정의	규칙이름						
내부 IP 주소	192.168.0.11	☐ 현재 접속된 PC의 IP주소로 설정(192.168.0.11)						
프로토콜	TCP	외부포트	80 ~ 80					
최대 60개의 규칙이 설정 가능합니다.		추가 취소						
낮은 번호일수록 우선순위가 높습니다.								
동작	☐	규칙이름	내부 IP	프로토콜	외부포트	내부포트	☐	삭제
1	☒	http	192.168.0.11	tcp	80	80	☐	
2	☒	ftp	192.168.0.11	tcp	21	21	☐	
3	☒	원격데스...	192.168.0.11	tcp	3389	3389	☐	

포트포워드 설정에 필요한 각각의 항목은 다음과 같습니다.

설정 항목	기능 설명
정의된 리스트	미리 정의된 규칙을 선택하거나 사용자가 임의로 정의 할 수 있습니다.
규칙이름	새로 입력하는 포트포워드 규칙의 이름을 입력합니다
내부IP주소	어플리케이션이 설치된 내부서버 또는 PC의 IP 주소를 입력합니다.
프로토콜	프로토콜의 종류를 선택합니다. (TCP 또는 UDP)
외부포트	외부 인터넷에서 접속시 사용되는 내부서버 또는 PC에 설치된 어플리케이션 포트범위를 설정합니다.
내부포트	내부서버 또는 PC에 설치된 어플리케이션 포트범위를 설정합니다 '외부포트'와 동일한 경우에는 입력하지 않아도 됩니다

- 위의 설정 예는 내부 IP 주소 192.168.0.11을 사용하는 PC의 HTTP 서버, FTP 서버 및 원격데스크톱 서비스를 외부 네트워크에서 접속 할 수 있도록 설정한 규칙 입니다.
- 먼저 입력된 낮은 번호의 규칙이 우선순위가 높습니다.
- 규칙이름을 클릭하시면 해당 규칙을 수정 할 수 있습니다.
- **동작** 체크박스를 해제하면 규칙은 남아 있으나 해당 규칙은 동작하지 않습니다.

8.2 포트트리거 설정



어플리케이션에서 사용하는 TCP/UDP 포트 번호를 감지하여 해당 어플리케이션에 필요한 포트를 현재 사용 중인 PC로 자동 포트포워딩 시켜주는 기능을 포트트리거 기능이라고 합니다.

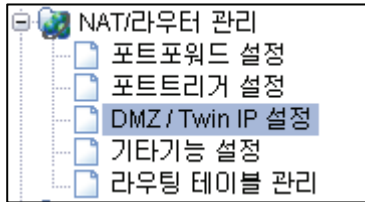
규칙이름			
포트트리거	프로토콜	TCP	
	포트범위	~	
포트포워드	프로토콜	TCP	
	포트범위		
최대 10개의 규칙이 설정 가능합니다. 추가			
규칙이름	포트트리거 조건	포트포워드 조건	☐ 삭제
1 트리거테스트	[tcp] 8080	[tcp] 80 8000 8001	☐

포트트리거 설정에 필요한 각각의 항목은 다음과 같습니다.

설정 항목	기능 설명
규칙이름	새로 입력하는 포트트리거 규칙의 이름을 입력합니다.
포트트리거-프로토콜	어플리케이션의 온라인 접속을 감지하기 위한 프로토콜의 종류를 선택합니다. 인터넷 어플리케이션 서버의 목적지 포트 프로토콜(TCP 또는 UDP 선택)
포트트리거-포트범위	어플리케이션의 온라인 접속을 감지하기 위한 포트범위를 입력합니다. 인터넷 어플리케이션 서버의 목적지 포트 번호
포트포워드-프로토콜	어플리케이션 사용을 위한 포트포워드 프로토콜의 종류를 선택합니다.
포트포워드-포트범위	어플리케이션 사용을 위한 포트포워드 포트를 입력합니다. 다수개의 포트 번호 입력시 구분은 "공백"으로 합니다.

- 위의 설정 예는 TCP 8080포트를 사용하는 외부 서버에 접속을 요청하는 내부 IP 주소로 TCP 80, 8000, 8001번 포트를 자동으로 포트포워드 설정하는 규칙입니다..
- 먼저 입력된 낮은 번호의 규칙이 우선순위가 높습니다.
- 포트포워드의 포트범위 입력시 구분은 '공백'으로 합니다.

8.3 DMZ/Twin IP 설정



DMZ 기능 또는 Twin IP 기능을 선택하여 설정 할 수 있습니다.

DMZ 설정

☐ 사용하지 않음
☒ **DMZ** (지정된 내부 IP주소의 PC로 모든 포트를 개방합니다. 단, 포트포워드에 설정된 포트는 제외)
☐ Twin IP (지정된 MAC주소의 PC가 공인 IP주소를 사용하도록 합니다)

내부 IP 주소: [192] [168] [0] [] ☐ 현재 접속된 PC의 IP주소로 설정(192.168.0.11)

포트포워드에 설정되어 있지 않은 모든 포트들을 내부의 특정 IP 주소를 가지는 PC로 개방 기능입니다. 어플리케이션 포트번호를 알 수 없어 인터넷 공유가 정상적으로 이루어지지 않는 프로그램들은 DMZ 호스트 기능으로 해결 할 수 있습니다.

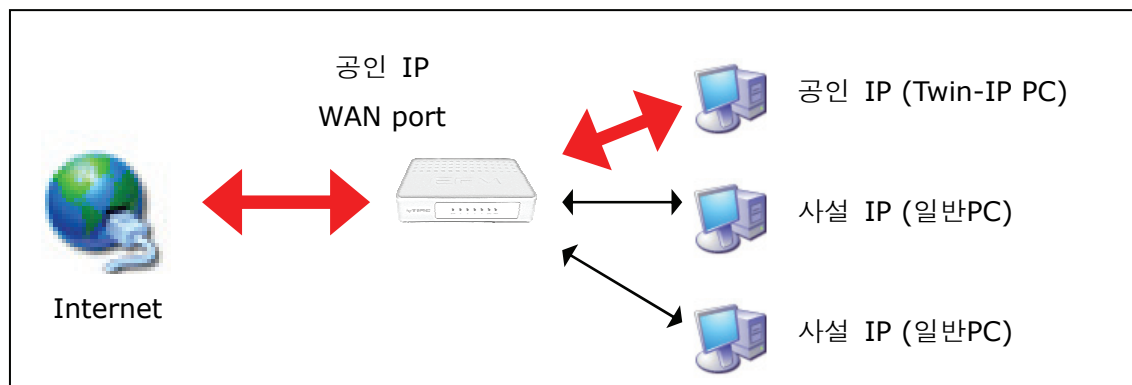
Twin IP 설정

☐ 사용하지 않음
☐ DMZ (지정된 내부 IP주소의 PC로 모든 포트를 개방합니다. 단, 포트포워드에 설정된 포트는 제외)
☒ **Twin IP** (지정된 MAC주소의 PC가 공인 IP주소를 사용하도록 합니다)

MAC 주소: ☐ 현재 접속된 PC의 MAC주소로 설정
 [] - [] - [] - [] - [] - []

IP 갱신 시간: [60] 초

Twin-IP는 인터넷 서비스 업체로 부여받는 공인 IP주소를 공유기와 연결된 내부의 특정 PC한대에 동시 설정하여 사용할 수 있는 기능입니다. 즉, Twin-IP기능이 설정된 PC의 경우에는 내부 사설 IP주소가 아닌 공인 IP주소를 가지고 공유기를 사용하지 않는 환경과 동일하게 인터넷을 이용하실 수 있는 기능입니다

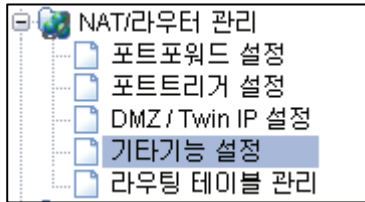


Twin-IP 설정 순서

- ① Twin-IP PC로 지정할 PC의 MAC 주소를 입력합니다.
- ② WAN의 IP 주소가 변경된 경우 IP 주소 갱신 시간이 지나면 Twin-IP PC의 IP 주소가 변경된 WAN IP 주소로 수정됩니다. 일반적인 경우 60초를 추천하며 WAN IP 주소가 바뀌게 되면 60초 이내에 Twin-IP PC로 변경된 IP 주소가 전달됩니다.
- ③ MAC 주소와 갱신 시간을 입력한 후 적용을 클릭합니다.
- ④ 설정 완료 후 해당 PC를 재시작하여야 Twin-IP 기능이 동작합니다.

■ Twin-IP 기능은 DHCP 서버가 동작 상태에서 사용 가능합니다.

8.4 기타기능 설정



FTP 비정규포트, 멀티캐스트 포워드, 인터넷 공유기능의 NAT 기타 기능을 설정 할 수 있습니다.

FTP 비정규포트

공유기 내부 또는 외부에 설치된 FTP 서버가 기본 포트 21번이 아닌 임의의 비정규 포트를 이용하여 운영되는 경우 FTP 비정규 포트 설정을 하여야 합니다

FTP 비정규포트	포트번호		추가
	☐ 2121 ☐ 0 ☐ 0 ☐ 0 ☐ 0	삭제	

- 2121번을 FTP 포트로 사용하는 경우에 설정한 예 입니다.

멀티캐스트 포워드

공유기의 내부와 외부간의 멀티캐스트 데이터들이 공유기의 동작과 무관하게 통신될 수 있도록 설정할 수 있습니다.

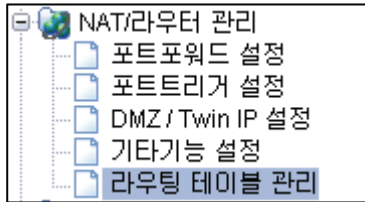
멀티캐스트 포워드	☐ 실행 ☒ 중단	적용
	멀티캐스트 데이터를 송수신하는 경우에 사용합니다.	

인터넷 공유 기능

인터넷 공유 기능을 중단시키면 공유기의 모든 기능이 중단되고 일반 라우터로 동작이 전환됩니다.

인터넷 공유 기능	☒ 실행 ☐ 중단	적용 후 시스템 재시작
	인터넷 공유 기능을 실행하거나 중단할 수 있습니다. 인터넷 공유 기능을 중단하면 관련된 기능이 자동으로 꺼집니다.	

8.5 라우팅 테이블 관리



라우팅 테이블 관리 기능은 라우팅 테이블을 직접 입력할 수 있게 하는 기능입니다

Type	Target	Mask	Gateway		
NET					
추가 가능한 최대 주소는 20개 입니다.					
추가					
Type	Target	Mask	Gateway	☐	삭제
1	NETWORK	192.168.10.0	255.255.255.0	192.168.0.20	☐

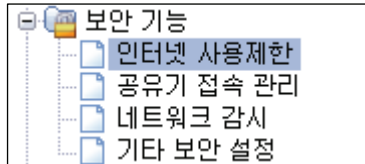
라우팅 테이블 설정에 필요한 각각의 항목은 다음과 같습니다.

설정 항목	기능 설명
Type	라우팅 테이블이 HOST 인지 NETWORK 인지를 설정합니다
Target	입력할 라우팅 테이블의 Target IP주소 또는 네트워크 주소를 입력합니다
Mask	Type이 NETWORK일 경우 Subnet mask를 결정합니다
Gateway	Target으로 통신할 때 거쳐갈 Gateway주소를 입력합니다

- 위의 설정 예는 192.168.10.0 network 을 목적지로 하는 모든 통신을 Gateway 192.168.0.20을 통하여 통신할 수 있도록 라우팅 테이블을 입력한 화면입니다.

9장 보안기능

9.1 인터넷 사용제한



IP 주소별/MAC 주소별로 인터넷을 차단/허용 할 수 있으며, 또는 어플리케이션의 포트 별로 인터넷을 차단/허용 할 수 있습니다. 설정방법은 `사용자 간단 설정`, `사용자 고급 설정`, `사이트 접속 차단 설정` 및 미리 등록된 어플리케이션

리스트(메신저, P2P, 게임)로 구분 됩니다. 그리고 각각 설정된 규칙들은 각각의 스케줄을 설정하여 정해진 요일과 시간에만 동작시킬 수 도 있습니다.

사용자 간단 설정 화면

입력방법 선택	사용자 간단 설정	규칙이름	
시작지 IP 주소	☒ 192.168.0.0 ~ 192.168.0.0 ☐ 모든 IP주소		
시작지 MAC 주소	☐ - - - - - MAC 주소 찾기		
허용/차단	차단	우선순위	

사용자 고급 설정 화면

입력방법 선택	사용자 고급 설정	규칙이름	
방향	내부 -> 외부		
시작지 IP 주소	☒ 192.168.0.0 ~ 192.168.0.0 ☐ 모든 IP주소		
시작지 MAC 주소	☐ - - - - - MAC 주소 찾기		
목적지 IP 주소	- - - - - ~ - - - - -		
프로토콜	-	목적지 포트	- ~ -
허용/차단	차단	우선순위	

사이트 접속 차단 설정 화면

입력방법 선택	사이트 접속 차단 설정	규칙이름	
시작지 IP 주소	☒ 192.168.0.0 ~ 192.168.0.0 ☐ 모든 IP주소		
시작지 MAC 주소	☐ - - - - - MAC 주소 찾기		
차단할 사이트 입력			
허용/차단	차단	우선순위	

사용자 스케줄 설정 화면

☒ 사용자 스케줄 설정하기	
스케줄-요일	☐ 일 ☐ 월 ☐ 화 ☐ 수 ☐ 목 ☐ 금 ☐ 토 ☐ 매일
스케줄-시간	00:00 ~ 00:00 24시간 타입 ☐ 24시간

- `사용자 스케줄 설정하기` 항목을 체크하지 않으면 해당 규칙은 요일/시간과 무관하게 무조건 적용됩니다.

인터넷 사용제한 설정에 필요한 각각의 항목은 다음과 같습니다.

설정 항목	기능 설명	비고
입력방법선택	`사용자 간단 설정`, `사용자 고급 설정`, `사이트 접속 차단 설정` 및 미리 등록된 어플리케이션 리스트(메신저, P2P, 게임)를 선택합니다.	공통
규칙이름	새로 입력하는 규칙의 이름을 입력합니다	공통
방향	내부->외부:공유기에 연결된 내부의 PC에서 외부로 통신 외부->내부:외부에서 공유기에 연결된 내부의 PC로 통신	고급
시작지 IP주소	내부->외부:내부PC의 IP 주소 (기본값) 외부->내부:외부PC의 IP 주소	공통
시작지 MAC 주소	내부->외부:내부PC의 MAC 주소 (기본값) 외부->내부:외부PC의 MAC 주소	공통
목적지 IP 주소	내부->외부:외부PC의 IP 주소 (기본값) 외부->내부:내부PC의 IP 주소	고급
프로토콜	TCP, UDP, ICMP를 선택합니다.	고급
목적지 포트	TCP, UDP 프로토콜을 선택 시 관련 목적지 포트번호를 입력합니다.	고급
차단할 사이트	접속을 차단하고자 하는 사이트의 문자열을 입력합니다 예를들어, 'sex hangame porn' 이라고 입력하시면 다음의 사이트들이 차단 됩니다. www.sex.com , www.sex.co.kr , www.hangame.com , www.hangame.co.kr , www.porn.com , www.porn.co.kr	사이트차단
우선순위	새로 입력하는 규칙을 우선순위를 지정합니다. 입력하지 않는 경우에는 최하위 우선순위로 설정됩니다.	공통
허용/차단	새로 입력하는 규칙을 허용할지 차단할지를 결정합니다. `사이트 접속 차단`의 경우에는 차단으로 고정됩니다.	공통

다음은 설정된 규칙 예제들 입니다.

낮은 번호일수록 우선순위가 높습니다.

동작	☐	규칙이름	스케줄	필터링 규칙	허용/차단	☐	삭제
1	☒	msm	월 화 수 목 금 09:00 ~ 18:00	필터링 규칙 보기	차단	☐	
[방향] 내부 -> 외부 [시작지 IP 주소] 모든 IP주소 [목적지 IP 주소] 모든 IP주소 [프로토콜 1] tcp 1863 [프로토콜 2] tcp 6891 ~ 6900 [차단할 사이트 입력] messenger.hotmail.com [차단할 사이트 입력] login.live.com							
2	☒	내부전용PC	매일 24시간	필터링 규칙 보기	차단	☐	
3	☒	차단사이트	매일 09:00 ~ 18:00	필터링 규칙 보기	차단	☐	

- 모든 IP 주소가 월~금, 09:00~18:00 사이에는 MSN 메신저를 접속하지 못하도록 차단한 예제 입니다.
- MSN 메신저의 경우에는 미리 등록된 어플리케이션 리스트에서 선택하면 됩니다.

낮은 번호일수록 우선순위가 높습니다.

동작	☐	규칙이름	스케줄	필터링 규칙	허용/차단	☐	삭제
1	☒	msm	월 화 수 목 금 09:00 ~ 18:00	필터링 규칙 보기	차단	☐	
2	☒	내부전용PC	매일 24시간	필터링 규칙 보기	차단	☐	
[방향] 내부 -> 외부 [시작지 IP 주소] 192.168.0.100 - 192.168.0.150 [목적지 IP 주소] 모든 IP주소							
3	☒	차단사이트	매일 09:00 ~ 18:00	필터링 규칙 보기	차단	☐	

- 192.168.0.100 ~ 192.168.0.150 사이의 IP주소를 사용하는 PC들은 항상 인터넷을 차단하도록 설정한 예제입니다.

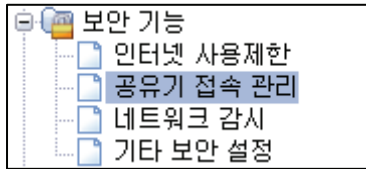
낮은 번호일수록 우선순위가 높습니다.

동작	☐	규칙이름	스케줄	필터링 규칙	허용/차단	☐	삭제
1	☒	msm	월 화 수 목 금 09:00 ~ 18:00	필터링 규칙 보기	차단	☐	
2	☒	내부전용PC	매일 24시간	필터링 규칙 보기	차단	☐	
3	☒	차단사이트	매일 09:00 ~ 18:00	필터링 규칙 보기	차단	☐	
[시작지 IP 주소] 모든 IP주소 [차단할 사이트 입력] naver daum empas							

- 모든 IP 주소가 매일 09:00 ~ 18:00 사이에는 naver, daum, empas 문자가 포함되는 모든 사이트에 접속하는 것을 차단하는 설정 예제 입니다.

- 먼저 입력된 낮은 번호의 규칙이 우선순위가 높습니다.
- **동작** 체크박스를 해제하면 규칙은 남아 있으나 해당 규칙은 동작하지 않습니다.
- `필터링 규칙 보기`를 클릭하셔야 자세한 필터링 규칙 정보를 볼 수 있습니다.

9.2 공유기 접속 관리



공유기 설정 웹 서버에 접속을 지정된 사용자만 가능하도록
설정 할 수 있습니다.

공유기 접속관리는 외부 접속과 내부 접속을 구분하여 관리합니다.

외부 접속 보안

외부 접속 보안	
☒ 원격 관리 포트 사용	5454
☒ 외부 접속 보안 사용	적용
허용 될 IP주소	
설명	추가
추가 가능한 최대 주소는 10개 입니다.	
IP주소	설명
1 210.198.10.200	사무실A

- 외부 접속을 위해서는 반드시 원격 관리 포트 번호를 지정하여야 합니다.
- 외부 접속 보안 사용을 체크하면 등록된 IP주소에서만 원격 관리 포트 번호를 통해서 공유기 설정 웹 서버로 접속할 수 있습니다.
- 유동 IP 서비스의 경우 외부 IP주소가 자주 바뀌기 때문에 DDNS 기능과 연동하여 사용하시면 편리합니다.

- 공유기의 접속은 웹 브라우저에 주소란에 **http://xxx.xxx.xxx.xxx:pppp**와 같이 URL을 입력하면 공유기 설정 화면에 접속이 가능합니다.(xxx.xxx.xxx.xxx : 외부 IP , pppp : 원격 관리 포트)
- 위의 예는 외부 IP 주소 210.198.10.200인 경우에만 원격 관리 포트 5454번을 통해 공유기 설정 웹 서버에 접속을 허용한 예제입니다.

내부 접속 보안

내부 접속 보안

☒ 내부 접속 보안 사용 적용

허용 될 IP주소

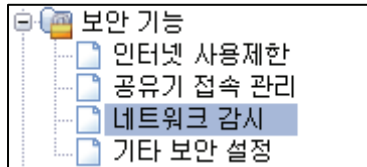
설명 추가

추가 가능한 최대 주소는 10개 입니다.

	IP주소	설명	☐	삭제
1	192.168.0.11	자동 항목	☐	
2	192.168.0.12	PC12	☐	

- 내부에서의 공유기 설정 웹 서버 접속은 기본적으로 공유기와 연결된 모든 PC에서 접속이 가능합니다.
- 내부 접속 보안을 사용을 체크하면 등록된 IP 주소에만 공유기 설정 웹 서버로 접속 할 수 있습니다.

9.3 네트워크 감시



악성 웹 바이러스나 P2P 프로그램의 경우 동시에 수천개의 인터넷 연결을 발생시켜 인터넷 회선을 마비시킬 수 있습니다. ipTIME의 네트워크 감시 기능은 이와 같은 통신 폭주 프로그램을 찾아내어 사용자에게 경고 메시지를 전달하고 폭주 프로그램의 통신을 적절히 제한하는 기능을 제공합니다.

네트워크 감시 설정				
동작 설정	☒ 실행 ☐ 중단 [바이러스 검사 페이지 접속하기]			
감시대상	☐ 알려진 웜바이러스 통신 ☒ 모든 통신			
감시수준	☒ 보통 ☐ 10 연결수/초			
감지된 통신차단	☒ 아니오 ☐ 웜바이러스 통신만 차단			
E-mail 통보정책	[관리자 E-mail을 설정] 하여야 E-mail 보고기능을 사용할수 있습니다.			
적용				
네트워크 감시 내역				
E-mail 바로 보내기			모든 감시 내역 삭제	
최근감지시간	IP 주소	프로토콜	감지횟수	설명 [적색:사용자 경고 해제상태]
2007/04/16 21:31:08	192.168.0.104	TCP/80	1	웹 과다 접속 감지 또는 웜바이러스 의심

네트워크 감시의 동작을 위하여 설정할 항목은 다음과 같습니다.

항목	설명						
동작 설정	실행 또는 중단 을 선택하여 네트워크 감시 동작을 설정합니다.						
감시 수준	<table border="1"> <tr> <td>낮음</td><td>초당 300개 이상의 동시 통신 감시</td></tr> <tr> <td>보통</td><td>초당 150개 이상의 동시 통신 감시</td></tr> <tr> <td>높음</td><td>초당 50개 이상의 동시 연결 감시</td></tr> </table> 감시 대상이 되는 통신 수준을 결정합니다. 사용자가 이 수치를 직접 정의할 수도 있으며 일반적으로 보통 수준의 감시 사용을 권장합니다. 설정된 수준을 넘어서는 통신이 감지되는 경우 로그를 기록하며 설정에 따라 초과하는 트래픽을 제한할 수 있습니다.	낮음	초당 300개 이상의 동시 통신 감시	보통	초당 150개 이상의 동시 통신 감시	높음	초당 50개 이상의 동시 연결 감시
낮음	초당 300개 이상의 동시 통신 감시						
보통	초당 150개 이상의 동시 통신 감시						
높음	초당 50개 이상의 동시 연결 감시						
감지된 통신 차단	감시 수준을 넘어서는 통신에 대해서 차단 여부를 결정합니다. 웜바이러스만 차단 옵션을 체크하면 바이러스 통신만을 차단합니다.						
E-mail 통보 정책	네트워크 감시의 감지 내역을 E-mail 통보하는 방법을 지정합니다.						

과도한 통신 트래픽이나 바이러스 트래픽이 유발 시키는 PC가 감지되면, 관리자에게 E-mail 보고와 로그 기록 이외에 해당 PC 사용자에게도 동일한 내용이 웹을 통해 보고됩니다. 해당 PC에서 웹 접속을 시도하는 경우에 '네트워크 감시'의 보고 페이지로 바뀌어 접속됩니다. 웹 보고 페이지는 다음과 같습니다.

보고서

바이러스검사

바이러스치료

항탈기

- 경고! 관리자가 정한 수준이상으로 인터넷을 사용하고 있습니다. 또는 웜바이러스에 감염되어 있을 수 도 있습니다.
- [경고해제/확인] 버튼을 클릭하셔야 정상적인 인터넷 사용이 가능합니다.
- [재경고해제]를 체크후 [경고해제/확인] 버튼을 클릭을 하시면 해당 이벤트 재발생시 경고페이지로 접속 되지 않습니다.
- 현재 정보는 <http://192.168.0.1/mypage.html> 에서 다시 확인하실 수 있습니다.

	최근감지시간	프로토콜	설명	재경고 해 제
NEW	2005/05/13 17:39:20	ICMP	해당포트 웜바이러스 감염 의심됨	☐
NEW	2005/05/13 17:38:06	TCP/80	웹 과다 접속 감지 또는 웜바이러스 의심	☐

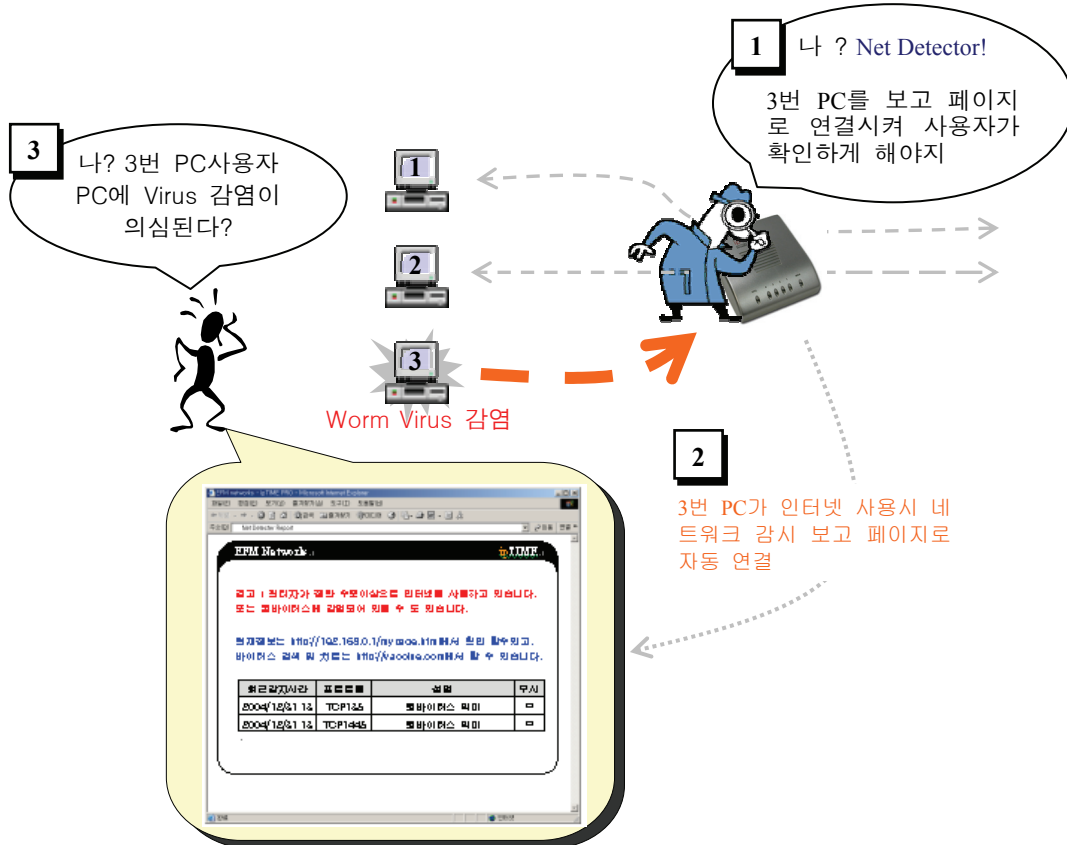
경고해제/확인

[무시] 항목을 체크하고 확인을 하는 경우에는, 해당되는 통신에 의해 트래픽이 감지되어도 웹 보고 페이지로 접속되지 않습니다. 단, 이외의 다른 통신에 의해 감지되는 경우에는 웹 보고 페이지로 접속이 됩니다. 관리자는 [모든 감시 내역 삭제]시에만 개인별 [무시]항목 설정을 해제 할 수 있습니다.

미리 정의된 웜 바이러스 또는 어플리케이션 통신 내용은 아래 표와 같습니다.

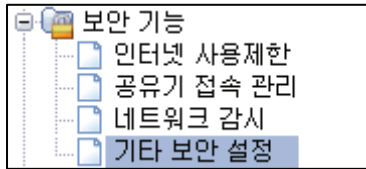
내용	통신 유형
SMTP 바이러스	TCP 25
Worm.Win32.Blaster / Win32 / Ralelka.worm 바이러스	TCP 135
Unknown worm 바이러스	TCP 139
Win32 / IRCBot.worm / Win32 / AgoBot.worm 바이러스	TCP 445
Worm.Win32.Welchina	TCP 707
Unknown worm 바이러스	UDP 137
SQL_Overflow 바이러스	UDP 1434
Unknown worm 바이러스	UDP 6677
소리 바다	TCP 7674 UDP 22321
당나귀	TCP 4662 UDP 4672
V-Share	TCP 8404 UDP 8402
Win-MX	TCP 6699
FileGuri	TCP 9493
KaZaA	TCP 3531 UDP 3531

- 네트워크 감시의 동작 개요는 다음과 같습니다.



- ① 사용자가 웹 설정 화면에서 네트워크 감시 기능을 활성화 하면 네트워크 감시 모듈은 PC에서 발생시키는 인터넷 통신 데이터를 분석한다.
- ② 특정 PC에서 인터넷을 마비 시킬 수준으로 통신을 발생 시키는 경우 웹 설정 화면과 특정 PC 사용자의 웹 화면으로 경고 메시지를 출력하고 사용자가 지정한 수준 이하로 해당 통신량을 제한하여 인터넷이 사용될 수 있게 한다.
- ③ 한 PC 사용자 또는 관리자는 웹 경고 화면에 따라 바이러스 존재 가능성을 확인할 수 있고, 연동되는 하우리 Live call 로 바이러스를 치료 할 수 있다.

9.4 기타 보안 설정



Denial of Service (DoS)는 한 사람이 공유자원을 모두 점유하여 다른 사람이 사용할 자원을 없애버리는 공격방식으로 해당 공격에 대해 방어설정을 할 수 있습니다.

기타 보안 설정	
SYN Flooding	☒ ON ☐ OFF TCP가 데이터를 보내기 전에 연결을 맺어야 하는 연결 지향(connection-oriented) 방식이라는 점을 착안하여 많은 수의 SYN bit이 설정 되어있는, 즉 연결을 요청하는 TCP 패킷을 호스트의 특정 포트에 보내어 포트의 대기 큐(backlog queue)를 가득차게 하여 포트에 들어오는 연결 요청을 큐가 빌 때 까지(connection time out이 될 때 까지) 무시하도록 하게 끔 하는 공격방식.
Smurf	☒ ON ☐ OFF ping의 목적지주소를 브로드캐스트 주소로 사용하는 공격방식. Smurf 공격은 Echo-request 패킷을 어떤 네트워크의 브로드캐스트 주소에 보내면 해당 네트워크의 모든 호스트가 request 패킷에 응답하느라 다른 일은 하지 못하도록 하는 공격 방식.
IP source routing	☒ ON ☐ OFF RFC 1122에 따르면 목적지의 경로에 대한 세부적인 내용을 담고 있는 IP Source Routing은 목적지 호스트에서도 같은 경로를 따라 반응을 해야 한다는 문제점이 있다. Cracker가 특정 네트워크에 Source Routing 패킷을 보낼 수 있다면 돌아오는 반응을 가로채서 상대방의 ? = 뭘??신뢰받은 호스트처럼 속일 수 있다.
IP Spoofing	☒ ON ☐ OFF 네트워크 시스템에서 서로 신뢰관계에 있는 A, B 두 시스템간에는 A 시스템의 account를 가지고 B 시스템을 액세스 할 수 있다. 이는 네트워크에서 신뢰관계를 형성하는 서비스가 네트워크 주소에 기반하여 이를 인증하기 때문이다. 이로 인해 IP Spoofing이 가능해진다. IP Spoofing은 이 신뢰관계에 있는 두 시스템사이에서 해커의 호스트를 마치 하나의 신뢰관계에 있는 호스트인 것처럼 속이는 것이다.
인터넷으로부터 오는 ICMP(ping) 막기	☒ ON ☐ OFF
인터넷으로 나가는 ICMP(ping) 막기	☒ ON ☐ OFF
적용	

(1) DoS 공격의 종류 및 설명

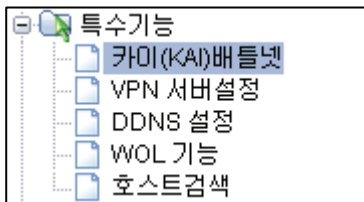
- ① SYN Flooding : TCP 가 데이터를 보내기 전에 연결을 맺어야 하는 연결 지향(connection-oriented) 방식이라는 점을 착안하여 많은 수의 SYN bit 이 설정 되어있는, 즉 연결을 요청하는 TCP 패킷을 호스트의 특정 포트에 보내어 포트의 대기 큐(backlog queue)를 가득차게 하여 포트에 들어오는 연결 요청을 큐가 빌 때 까지(connection time out 이 될 때 까지) 무시하도록 하게 끔 하는 공격방식.

- ② **Smurf** : ping 의 목적지주소를 브로드캐스트 주소로 사용하는 공격 방식. Smurf 공격은 Echo-request 패킷을 어떤 네트워크의 브로드캐스트 주소로 보내면 해당 네트워크의 모든 호스트가 request 패킷에 응답하느라 다른 일은 하지 못하도록 하는 공격방식.
- ③ **IP Source Routing** : RFC 1122 에 따르면 목적지의 경로에 대한 세부적인 내용을 담고 있는 IP Source Routing 은 목적지 호스트에서도 같은 경로를 따라 반응을 해야 한다는 문제점이 있다. Cracker 가 특정 네트워크 Source Routing 패킷을 보낼 수 있다면 돌아오는 반응을 가로채서 상대방의 호스트와 신뢰받은 호스트처럼 속일 수 있다.
- ④ **IP Spoofing** : 네트워크 시스템에서 서로 신뢰관계에 있는 A, B 두 시스템간에는 A 시스템의 account 를 가지고 B 시스템을 액세스 할 수 있다. 이는 네트워크에서 신뢰관계를 형성하는 서비스가 네트워크 주소에 기반하여 이를 인증하기 때문이다. 이로 인해 IP Spoofing 이 가능해 진다. IP Spoofing 은 이 신뢰관계에 있는 두 시스템 사이에서 Hacker 의 호스트를 마치 하나의 신뢰관계에 있는 호스트인 것처럼 속이는 것이다.
- ⑤ 인터넷으로부터 오는 ICMP(ping) 막기를 설정하면 공유기는 인터넷에서 수신되는 Ping 요청에 응답하지 않습니다.
- ⑥ 인터넷으로 나가는 ICMP(ping) 막기를 설정하면 공유기에 연결된 PC 가 송신하는 모든 Ping 요청을 차단하여 공유기에 연결된 PC 는 공유기에 대한 ping 과 인터넷에 존재하는 다른 장비에 대한 ping 시험을 할 수 없게 됩니다. 이 기능을 설정하면 바이러스에 걸린 내부 PC 가 과도한 ping 요청으로 공유기와 인터넷에 존재하는 다른 장비를 공격하는 것으로 보호해줍니다.

10장 특수기능

10.1 카이(KAI)배틀넷

해당 기능은 무선 AP기능이 제공되는 ipTIME 유무선 공유기 일부 제품에서만 지원합니다.

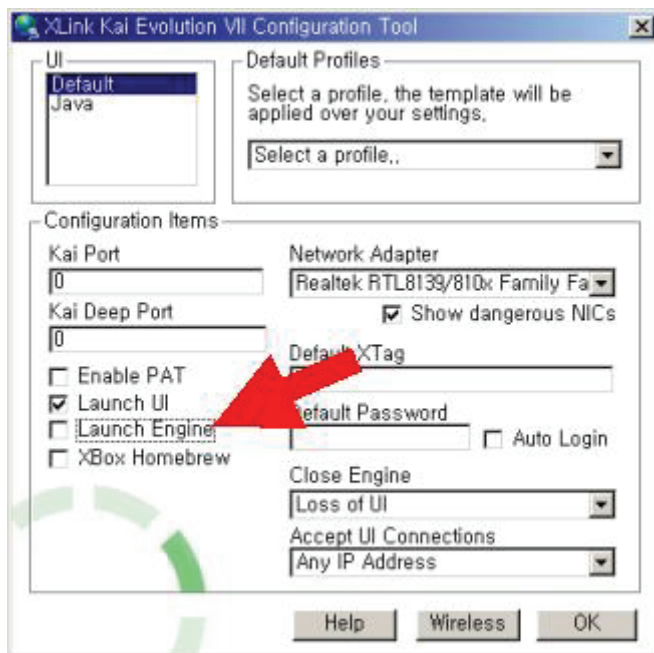


카이 배틀넷 기능을 사용하면, PSP에서 지원되는 대전기능을 이용하여 인터넷상의 다른 사용자와 게임을 즐길 수 있습니다.

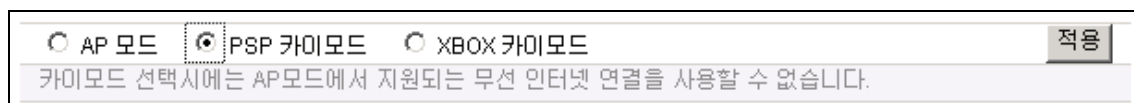
주의> 카이배틀넷 기능을 사용하면 무선 AP기능을 사용할 수 없습니다.

카이 이용방법

- ① 카이 가입하기 - www.teamxlink.co.uk 에서 가입
 - ② PSP 카이 프로그램을 유선PC에 설치하기 - www.teamxlink.co.uk 에서 다운로드
 - ③ KAI Config Tool 실행 후 PC에서 사용될 Launch Engine 끄기 (공유기의 KAI엔진 이용)
- [카이 Config Tool 실행화면]



- ④ PSP에서 해당 타이틀의 넷대전 모드로 게임 실행
- ⑤ PSP의 무선랜 LED(좌측 하단)가 깜박거리는지 확인)
- ⑥ 공유기에서 PSP카이모드로 전환



⑦ 게임서버를 선택 후, 아래의 그림처럼 게임기가 검색되는지 확인

KAI 엔진 상태	정상적으로 실행됨	KAI엔진 포트번호 37500	KAI엔진 재시작
게임기 검색	PSP 검색됨	받은 패킷 [5191], 보낸 패킷 [24] 동적 SSID 변경 기능 동작중	
	Game	Tekken - Dark Resurrection	
	ESSID	PSP_AULJS00048_L_PBLBY00	
	BSSID	02:7B:3E:34:0E:86	
	Channel	6	
	PSP MAC	00:01:4A:1F:21:4D	
	채널 선택	AUTO	
	☐ PSP MAC 머드레스 등록(게임기검색실패시 입력)	- - - - -	
		게임기 검색	
Tekken - Dark Resurrection	Dynamic SSID Change 라는 기술을 통해 지원. 다른 일반 무선 랜카드 사용자와는 게임을 할 수 없을 수도 있습니다.		
카이 서버 변경	카이 서버 변경		

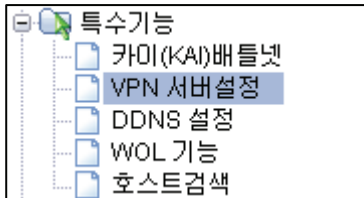
* 검색 실패 시에는 PSP MAC주소를 등록한 후 게임기를 재검색 합니다.

⑧ 카이UI 프로그램을 실행하여 해당 게임 방 접속 후, 게임 시작.

보다 자세한 사용방법은 www.iptime.co.kr 의 [고객지원](#) >> [네트워크](#) >> [기술자료](#) 게시판에서 확인하시기 바랍니다.

10.2 VPN 서버설정

해당 기능은 제품 모델에 따라 지원되지 않을 수 있습니다.



VPN 서버 기능을 이용하면 인터넷에 연결된 다수의 PC를 하나의 LAN에 연결된 것처럼 망을 구성할 수 있습니다.

VPN 서버에 연결된 PC 사이에 자유롭게 파일 공유 및 프린터 공유를 할 수 있으며 LAN 환경에서 사용되는 여러 프로그램들을 자유롭게 사용할 수 있습니다.

- ipTIME의 VPN 서버 기능은 최대 5명의 사용자까지 VPN 서버에 접속하여 LAN VPN 환경을 구성할 수 있습니다.
- VPN 서버에 접속하기 위해서는 해당 PC의 윈도우 운영 체제에서 가상 사설망 접속 어댑터를 설치하여야 합니다.

VPN(PPTP) 서버설정

동작 설정

☒ 실행 ☐ 중단

암호화(MPPE)

☒ 암호화 사용함 ☐ 암호화 없음

적용

VPN(PPTP) 계정 설정

VPN 접속 계정

VPN 접속 암호

할당될 IP 주소

192.168.0.0

최대 5명의 사용자를 추가 할 수 있습니다.

추가

VPN 접속 계정	할당될 IP 주소	연결 상태	연결끊기	삭제
vpnuser1	192.168.0.107	연결되지않음	☐	☐
vpnuser2	192.168.0.108	접속됨	☐	☐

VPN 서버 설정을 위하여 설정할 항목은 다음과 같습니다.

항목	설명
동작 설정	실행 또는 중단 을 선택하여 VPN 기능 동작을 설정합니다.
암호화(MPPE)	MPPE 암호화 사용여부를 선택합니다.
VPN 접속 계정	VPN을 사용할 새로운 계정을 입력합니다.
VPN 접속 암호	VPN을 사용할 새로운 계정의 암호를 입력합니다.
할당할 IP 주소	VPN을 사용할 새로운 계정이 할당 받을 IP 주소를 지정합니다.

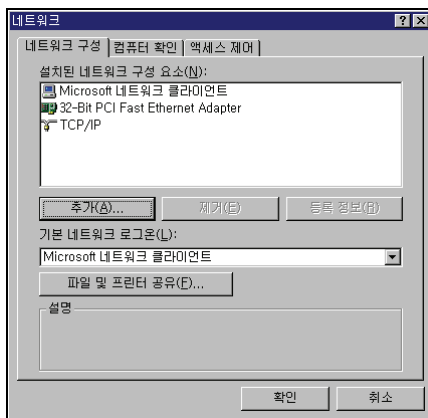
[참고] VPN을 구성하는 방법은 IPSec 또는 PPTP 등의 방법이 있으며, ipTIME은 PPTP 기반의 VPN을 지원한다.

10.2.1 Windows 98/ME에서의 VPN 서버 접속

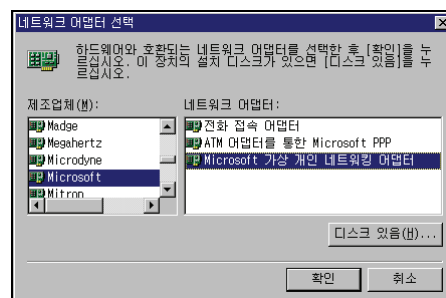
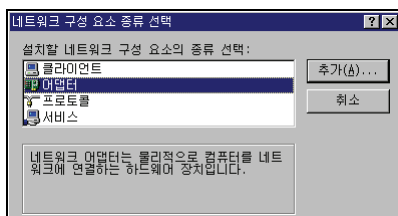
VPN 서버에 접속하여 가상 사설망을 구축하기 위해서는 먼저 가상 사설망 어댑터를 설치합니다. 가상 사설망 어댑터는 윈도우 운영 체제에서 제공됩니다. 가상 사설망 이용을 위해서는 다음 (1) 의 설정을 진행하여야 하며 한번 설정이 완료된 이후에는 (2) 접속 방법을 통하여 연결하면 된다.

(1) 가상 사설망 어댑터 설치

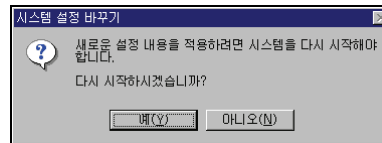
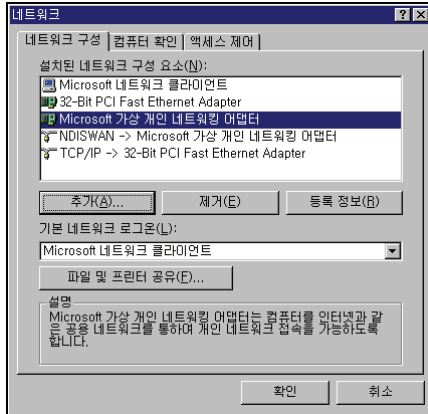
- 윈도우 바탕 화면의 네트워크 환경을 마우스 우측 버튼으로 클릭한 뒤 “등록 정보”를 선택합니다.
- VPN 어댑터 추가를 위하여 추가 버튼을 클릭합니다.



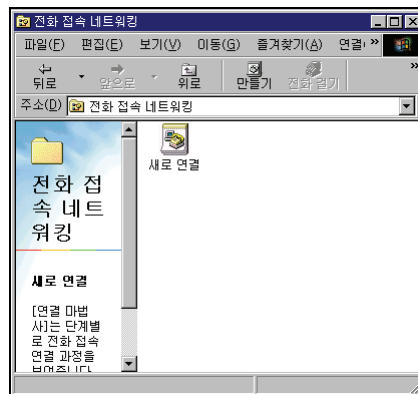
- 네트워크 구성 요소 중 어댑터를 선택한 뒤 추가 버튼을 클릭하여 Microsoft의 VPN 어댑터를 선택합니다.



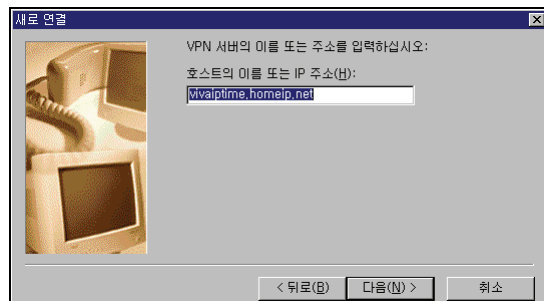
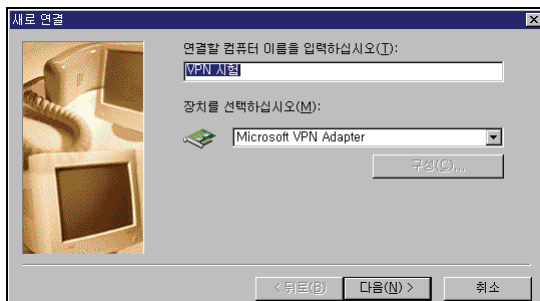
- 확인을 선택하면 가상 개인 네트워킹 어댑터가 추가된 것을 확인할 수 있고 확인을 클릭하면 시스템이 재 시작됩니다.



- 시스템이 재 시작된 뒤 바탕 화면의 내 컴퓨터를 더블 클릭하고 이 중 전화 접속 네트워킹을 클릭합니다.

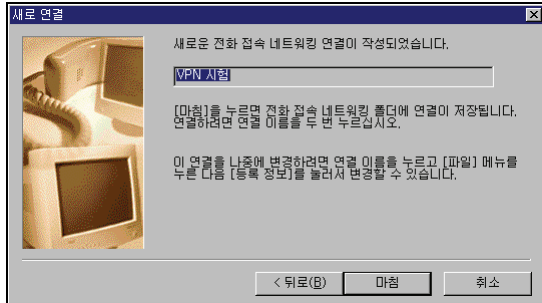


- 새로 연결을 구성하고자 하는 VPN망의 이름과 VPN 서버의 주소를 입력합니다.



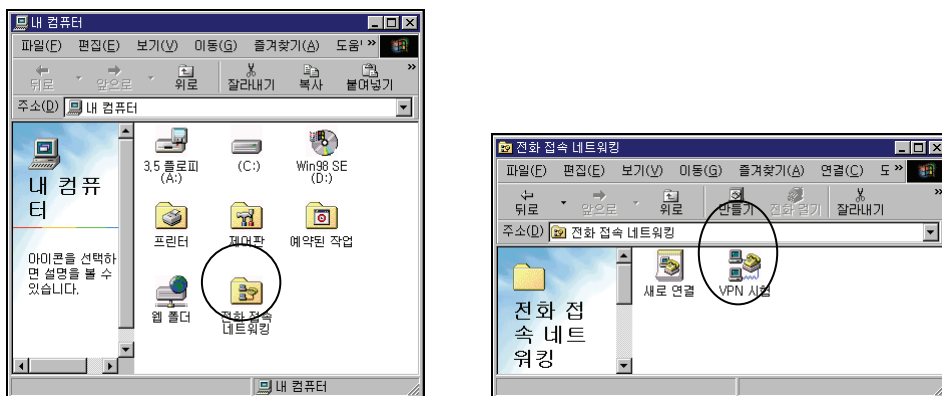
[참고] VPN 망 이름은 임의로 자유롭게 입력할 수 있으면 DDNS를 사용하면 DNS 이름으로 공유기에 접근할 수 있어 편리합니다.

- 마침을 클릭하여 VPN 구성을 완료 합니다.

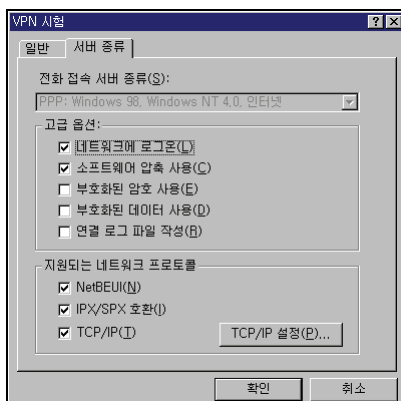


(2) 가상 사설망 어댑터의 옵션 조절

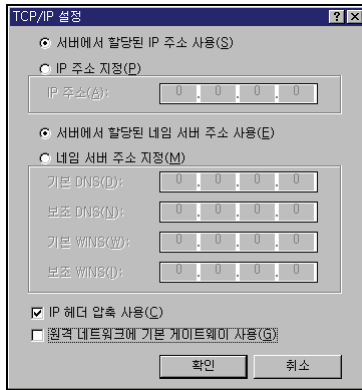
- 바탕 화면의 내 컴퓨터를 더블 클릭하고 이 중 전화 접속 네트워킹을 마우스 우측 버튼으로 클릭하여 등록 정보를 선택합니다.



- 서버 종류 항목을 선택하여 암호와 관련 옵션을 조정한다. 공유기 설정에서 암호화 (MPPE)를 사용하는 것으로 설정하였다면, "부호화된 데이터 사용"에 체크합니다.



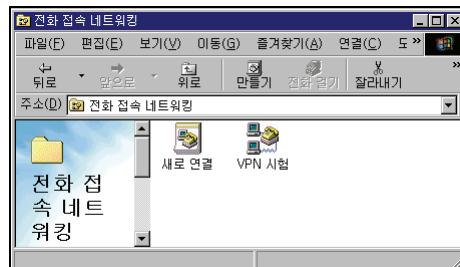
- TCP/IP 설정을 선택하여 원격네트워크 기본 게이트웨이 사용이 체크되지 않도록 합니다.



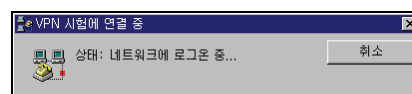
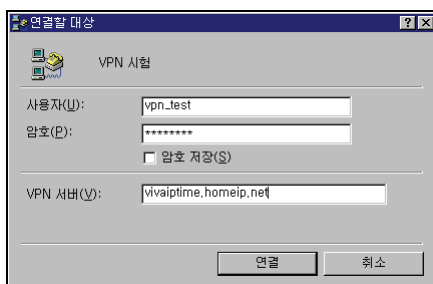
- 확인을 클릭하여 등록 정보 수정을 완료합니다.

(2) VPN 접속

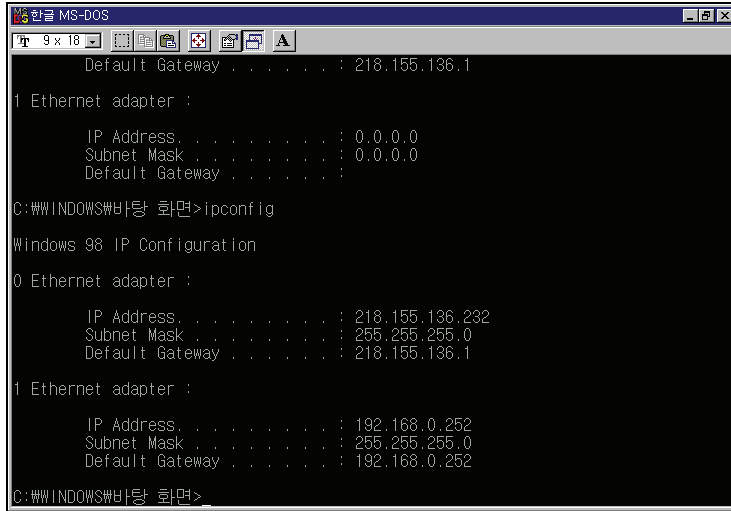
- VPN 접속을 위해서 바탕 화면의 내 컴퓨터를 더블 클릭하고 이 중 전화 접속 네트워킹을 클릭합니다.



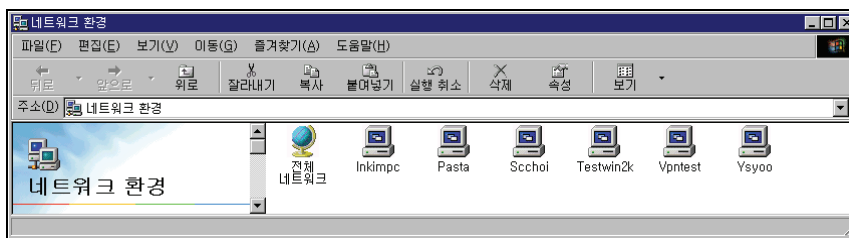
- 새로 생성된 VPN 접속 아이콘을 클릭하여 VPN 사용자 계정과 암호를 입력하면 VPN 접속이 완료됩니다.



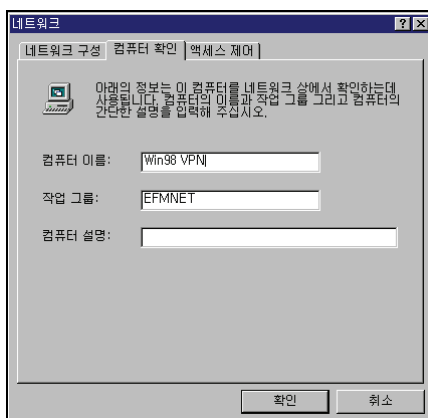
- VPN 접속 상태는 명령 프롬프트의 ipconfig 명령으로 확인할 수 있습니다.



- 네트워크 환경을 검색하면 가상 사설망 LAN으로 연결된 PC를 확인할 수도 있습니다.



[참고] VPN 접속 시 LAN 상의 모든 자원을 자유롭게 공유하기 위해서는 네트워크 환경에서 작업 그룹을 연결하고자 하는 VPN 망의 작업 그룹과 동일하게 설정하여야 합니다.

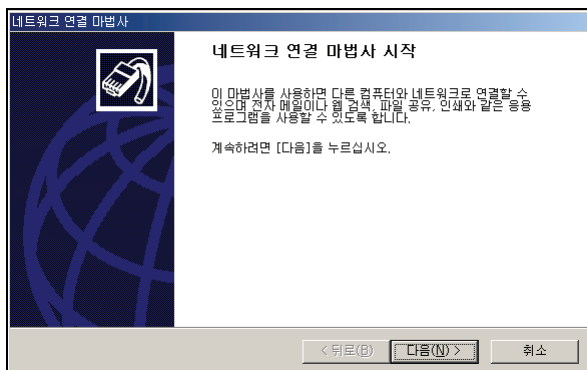


10.2.2 Windows 2000에서의 VPN 서버 접속

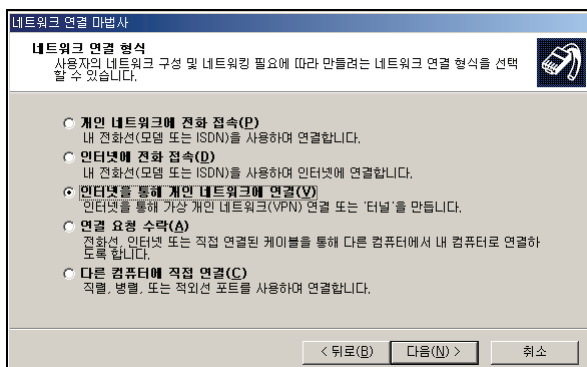
VPN 서버에 접속하여 가상 사설망을 구축하기 위해서는 먼저 가상 사설망 어댑터를 설치합니다. 가상 사설망 어댑터는 윈도우 운영 체제에서 제공됩니다. Windows 2000 운영 체제에서 가상 사설망 이용을 위해서는 다음 (1) ~ (3)까지의 설정을 진행하여야 하며 한번 설정이 완료된 이후에는 (4) 접속 방법을 통하여 연결합니다.

(1) 가상 사설망 어댑터 설치

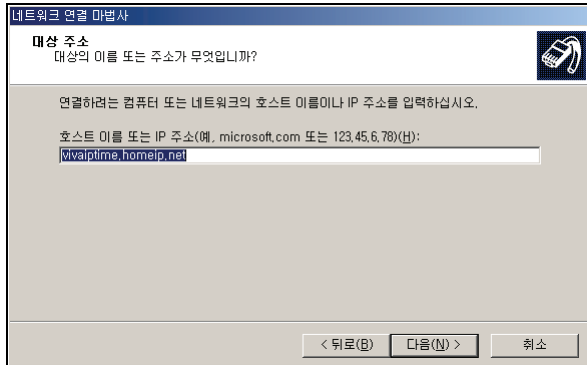
- 윈도우 시작 버튼을 클릭하여 **설정>>네트워크 및 전화 접속 연결>>새 연결 만들기**를 선택한 후 네트워크 연결 마법사가 실행되면 다음을 클릭합니다.



- 네트워크 연결 형식은 VPN을 선택한 후 다음을 클릭합니다.

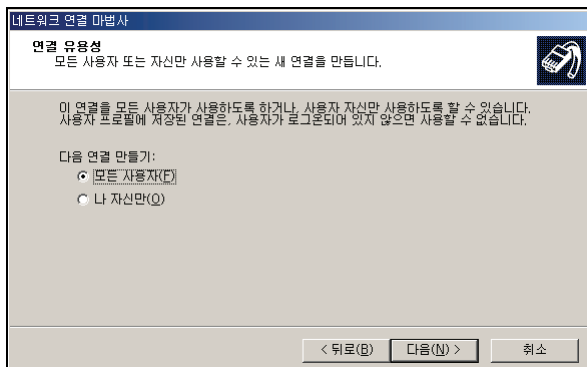


- 연결하고자 하는 VPN 서버 (공유기)의 주소를 입력한 후 다음을 클릭합니다.



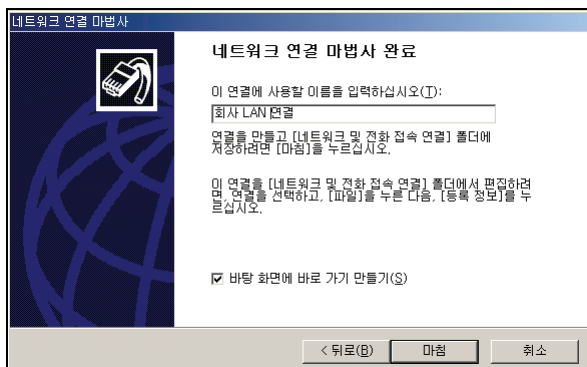
[참고] DDNS를 사용하면 DNS 이름으로 공유기에 접근할 수 있어 편리합니다.

- 설치된 가상 사설망 어댑터를 사용할 수 있는 사용자를 선택한 후 다음을 클릭합니다.



[참고] 별도의 사용자 관리를 하지 않는 경우 모든 사용자를 선택합니다.

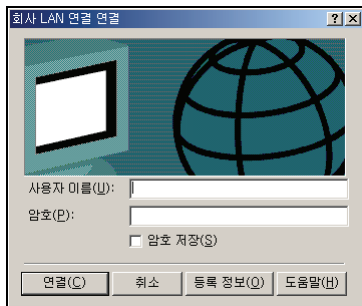
- 설치된 가상 사설망의 이름을 입력하고 확인을 클릭하면 어댑터 설치가 완료됩니다.



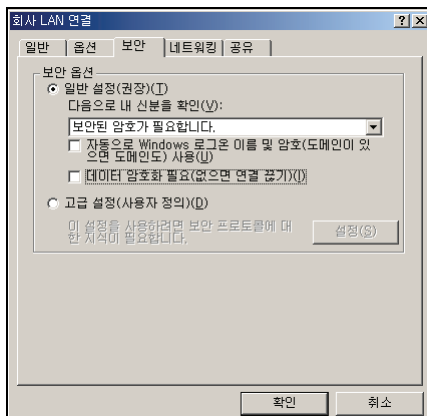
[참고] 사설망의 이름은 임의로 입력하면 되며 하단의 단축 아이콘 생성 옵션을 선택하면 바탕 화면에 가상 사설망 접속 아이콘이 생성됩니다.

(2) 가상 사설 망 어댑터의 옵션 조정

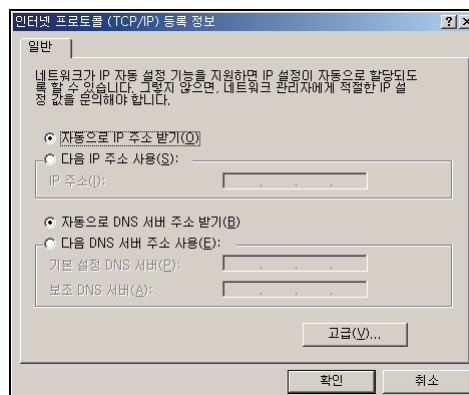
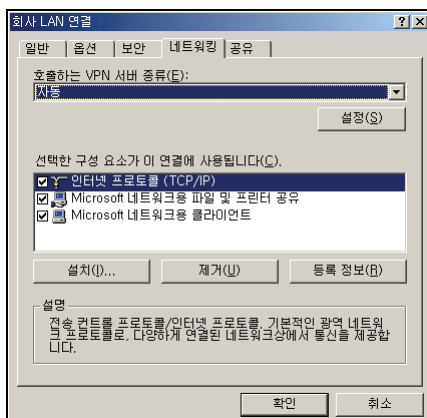
- 가상 사설망 어댑터 접속 프로그램이 실행되면 등록 정보 버튼을 클릭합니다.



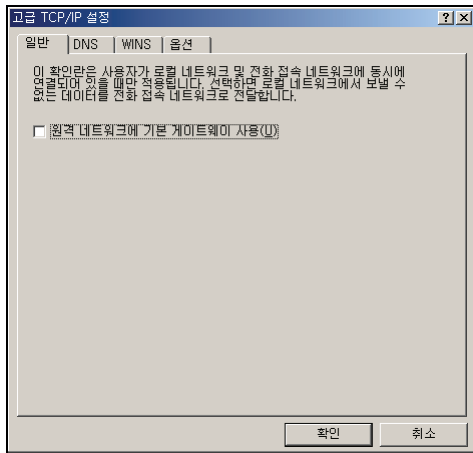
- 보안 항목을 설정하며 "데이터 암호화 필요"의 체크 상태를 확인합니다. 만약, 공유기의 설정에서 암호화 (MPPE)를 사용하는 것으로 설정하였다면, "데이터 암호화필요"에 체크를 하셔야 됩니다.



- 네트워크 항목 중 TCP/IP 항목을 더블 클릭합니다.



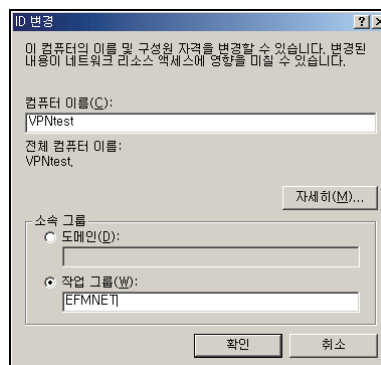
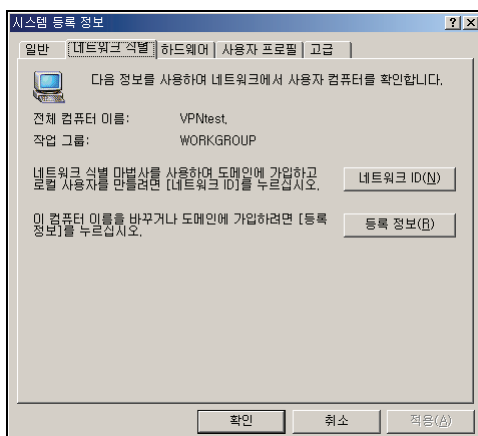
- 고급 버튼을 클릭하여 원격 네트워크에 기본 게이트웨이 사용에 체크가 해제되었는지 확인합니다.



- 암호화 설정과 원격 게이트웨이에 대한 설정을 확인한 뒤 확인 버튼을 클릭하여 등록 정보 창을 닫습니다.

(3) 워크 그룹 이름의 확인

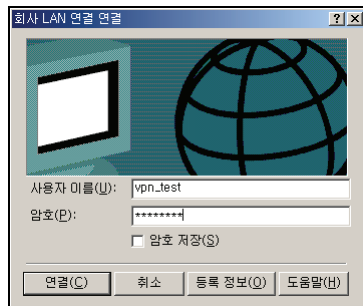
- VPN 서버에 접속한 뒤 정상적인 윈도우 공유 시스템을 위해서는 LAN 환경에 PC 및 가상 사설망으로 접속하는 모든 PC는 동일한 워크 그룹 이름을 갖고 있어야 합니다.
- 컴퓨터의 워크 그룹 이름 변경을 위하여 바탕 화면의 내 컴퓨터를 마우스 우측 버튼으로 클릭한 뒤 등록 정보를 클릭하고 네트워크 식별 항목을 선택하고 등록 정보 버튼을 클릭합니다.
- 작업 그룹 이름을 가상 사설망으로 연결하고자 하는 LAN의 그룹 이름과 동일하게 수정합니다.



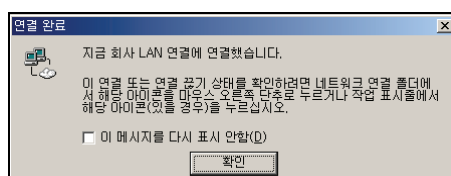
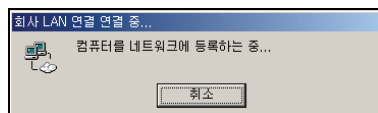
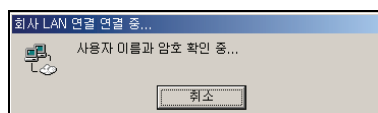
[참고] 워크 그룹 이름이 다른 경우 윈도우 환경에서 공유가 정상적으로 수행되지 않습니다.

(4) VPN 접속

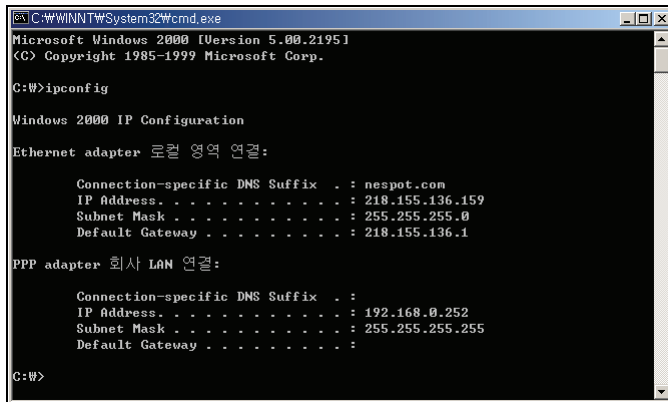
- 바탕 화면의 단축 아이콘 또는 네트워크 등록 정보의 가상 사설망 어댑터 아이콘을 클릭합니다.
- 가상 사설 망 연결 프로그램이 실행되면 등록된 사용자 이름과 암호를 입력한 뒤 연결을 클릭합니다.



- VPN 서버와 정상으로 접속되는 경우 아래와 같은 메시지가 표시됩니다.



- VPN 접속 상태는 명령 프롬프트의 ipconfig 명령으로 확인할 수 있습니다.



```
C:\WINNT\System32\cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\W>ipconfig

Windows 2000 IP Configuration

Ethernet adapter 로컬 영역 연결:

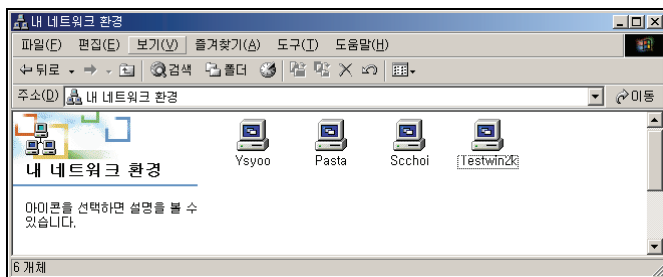
    Connection-specific DNS Suffix  . : nespot.com
    IP Address. . . . . : 218.155.136.159
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 218.155.136.1

PPP adapter 회사 LAN 연결:

    Connection-specific DNS Suffix  . :
    IP Address. . . . . : 192.168.0.252
    Subnet Mask . . . . . : 255.255.255.255
    Default Gateway . . . . . :

C:\W>
```

- 또 네트워크 환경을 검색하면 가상 사설망을 통하여 LAN으로 연결된 PC를 확인할 수도 있습니다.



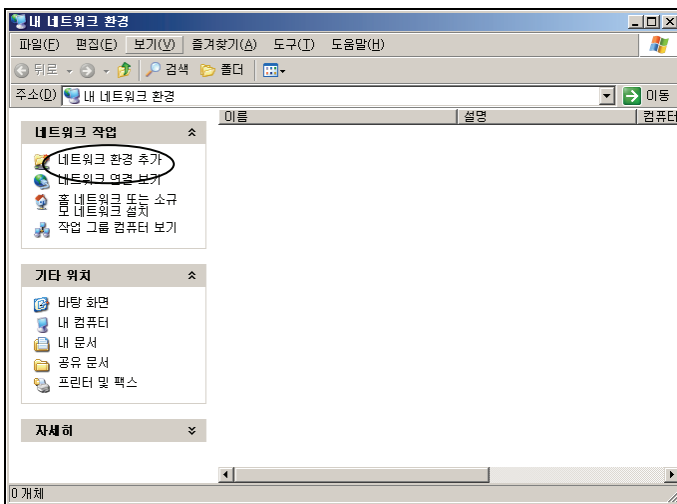
- VPN 서버와 연결이 완료되면 LAN 상의 모든 자원을 자유롭게 공유할 수 있습니다.

10.2.2 Windows 2000에서의 VPN 서버 접속

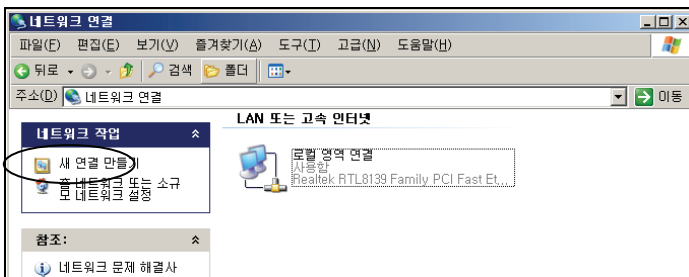
VPN 서버에 접속하여 가상 사설망을 구축하기 위해서는 먼저 가상 사설망 어댑터를 설치합니다. 가상 사설망 어댑터는 윈도우 운영 체제에서 제공됩니다. 가상 사설망 이용을 위해서는 다음 (1) ~ (3)까지의 설정을 진행하여야 하며 한번 설정이 완료된 이후에는 (4) 접속 방법을 통하여 연결합니다.

(1) 가상 사설망 어댑터 설치

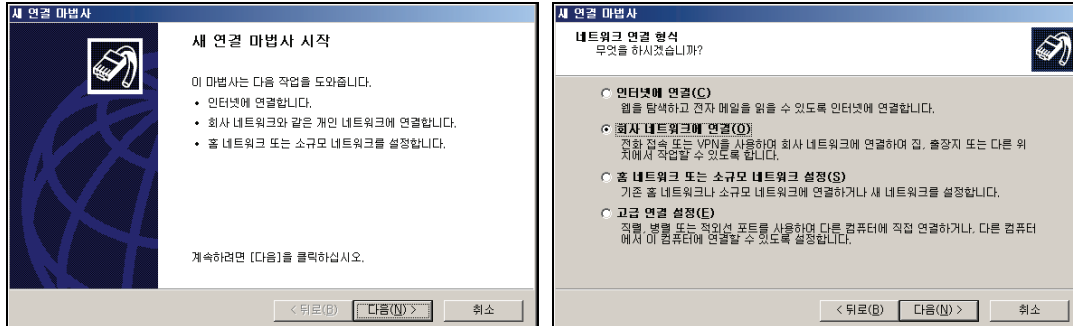
- 윈도우 [시작] 버튼을 클릭하여 [내 네트워크 환경]을 선택한 뒤 [네트워크 연결 보기]를 선택합니다.



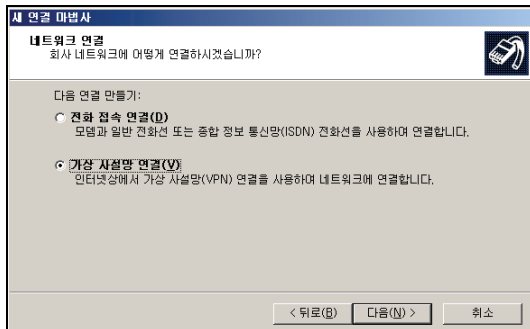
- 새 연결 만들기를 클릭하여 새 연결 마법사를 실행합니다.



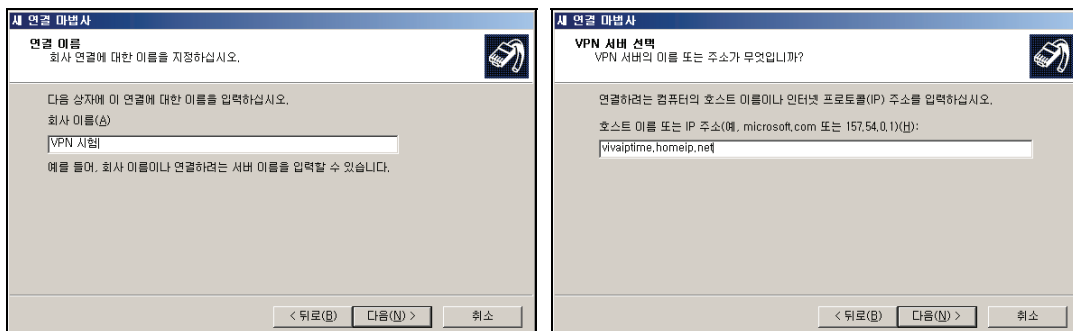
- 네트워크 연결 마법사가 실행되면 다음을 클릭하고 연결 형식에서는 회사 네트워크 연결을 선택합니다.



- 네트워크 연결 방법은 VPN 연결을 선택합니다.

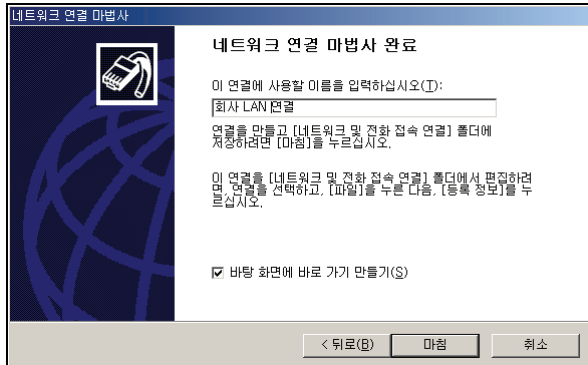


- VPN 망의 이름을 입력한 뒤 접속하고자 하는 VPN 서버 (공유기)의 주소를 입력합니다.



[참고] VPN 망 이름은 임의로 자유롭게 입력할 수 있으면 DDNS를 사용하면 DNS 이름으로 공유기에 접근할 수 있어 편리합니다.

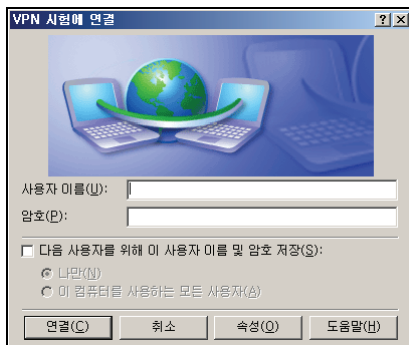
- 마지막으로 마침을 클릭하면 가상 사설망 어댑터 설치가 완료됩니다.



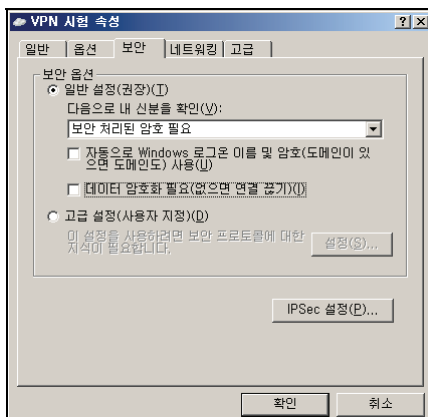
[참고] 단축 아이콘 생성 옵션을 선택하면 바탕화면에 접속 아이콘이 생성됩니다.

(2) 가상 사설 망 어댑터의 옵션 조정

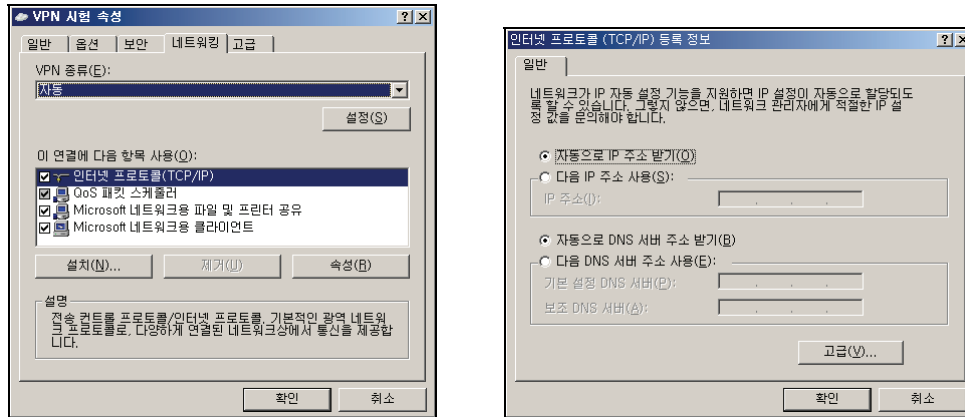
- 가상 사설망 어댑터 접속 프로그램이 실행되면 속성 버튼을 클릭합니다.



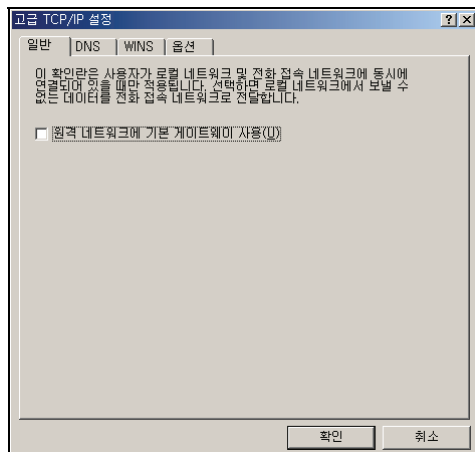
- 보안 항목을 설정하며 “데이터 암호화 필요”의 체크상태를 확인합니다. 공유기의 설정에서 암호화 (MPPE)를 사용하는 것으로 설정하였다면, “데이터 암호화필요”에 체크를 하여야 합니다.



- 네트워크 항목 중 TCP/IP 항목을 더블 클릭합니다.



- 고급 버튼을 클릭하여 원격 네트워크에 기본 게이트웨이 사용에 체크가 해제되었는지 확인합니다.

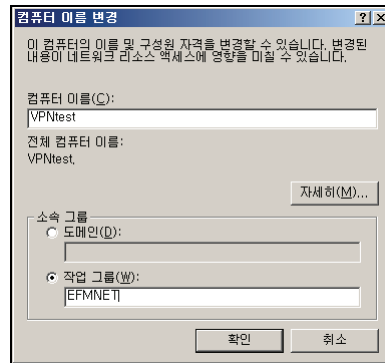
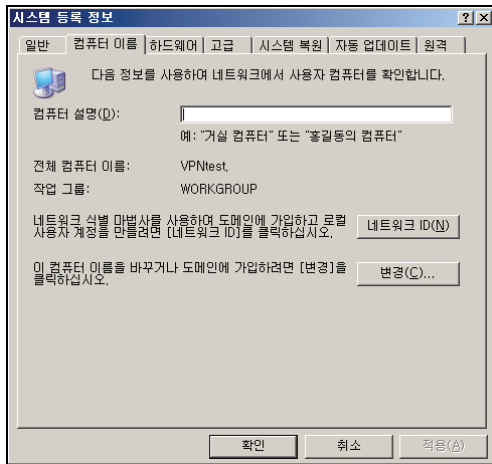


- 암호화 설정과 원격 게이트웨이에 대한 설정을 확인한 뒤 확인 버튼을 클릭하여 등록 정보 창을 닫습니다.

(3) 워크 그룹 이름의 확인

- VPN 서버에 접속한 뒤 정상적인 윈도우 공유 시스템을 위해서는 LAN 환경에 PC 및 가상 사설망으로 접속하는 모든 PC는 동일한 워크 그룹 이름을 갖고 있어야 합니다.
- 컴퓨터의 워크 그룹 이름 변경을 위하여 시작 메뉴의 내 컴퓨터를 마우스 우측 버튼으로 클릭한 뒤 속성을 클릭하고 컴퓨터 이름 항목을 선택하고 변경 버튼을 클릭합니다.

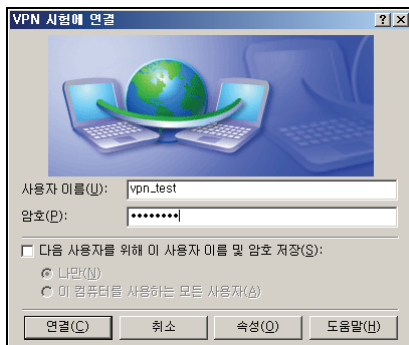
- 작업 그룹 이름을 가상 사설망 LAN의 그룹 이름과 동일하게 합니다.



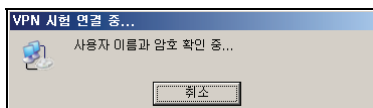
[참고] 워크 그룹 이름이 다른 경우 윈도우 환경에서 공유가 정상적으로 수행되지 않습니다.

(4) VPN 접속

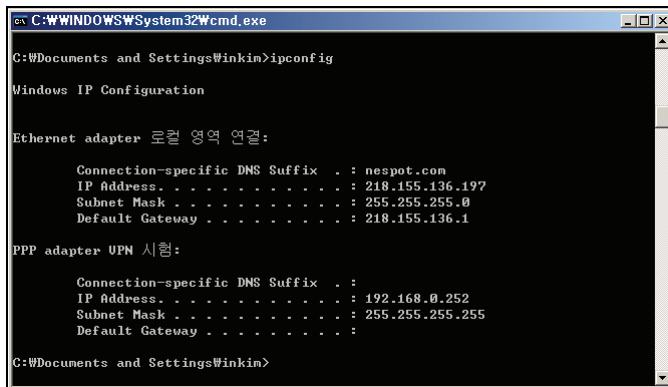
- 바탕 화면의 단축 아이콘 또는 네트워크 등록 정보의 가상 사설망 어댑터 아이콘을 클릭합니다.
- 가상 사설 망 연결 프로그램이 실행되면 등록된 사용자 이름과 암호를 입력한 뒤 연결을 클릭합니다.



- VPN 서버와 정상으로 접속되는 경우 아래와 같은 메시지가 표시됩니다.



- VPN 접속 상태는 명령 프롬프트의 ipconfig 명령으로 확인할 수 있습니다.



```

C:\WINDOWS\System32\cmd.exe
C:\Documents and Settings\Winkin>ipconfig

Windows IP Configuration

Ethernet adapter 로컬 영역 연결:

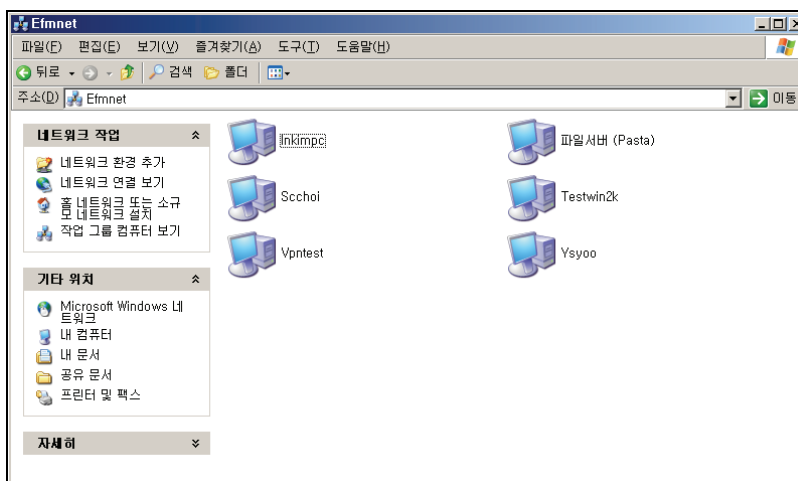
    Connection-specific DNS Suffix  . : nespot.com
    IP Address. . . . . : 218.155.136.197
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 218.155.136.1

PPP adapter VPN 시험:

    Connection-specific DNS Suffix  . :
    IP Address. . . . . : 192.168.0.252
    Subnet Mask . . . . . : 255.255.255.255
    Default Gateway . . . . . :

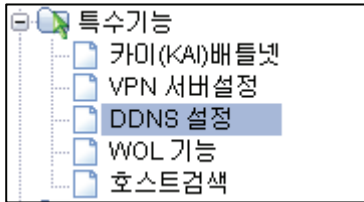
C:\Documents and Settings\Winkin>
  
```

- 네트워크 환경을 검색하면 가상 사설망을 통하여 LAN으로 연결된 PC를 확인할 수도 있습니다.



- VPN 서버와 연결이 완료되면 LAN 상의 모든 자원을 자유롭게 공유할 수 있습니다.

10.3 DDNS 설정



유동 IP 주소에 도메인 이름을 지정하여 고정 IP 주소처럼 사용할 수 있습니다.

DDNS을 사용하면 매번 공유기의 외부 IP주소를 확인하지 않아도 편리하게 서버 운영을 할 수 도 있습니다

- ipTIME에서는 ipTIME DDNS와 DynDNS를 지원합니다.
- ipTIME DDNS를 사용하기 위해서는 별도의 등록 절차 없이 공유기 설정만으로 사용할 수 있습니다.
- DynDNS 설정을 위해서는 먼저 www.dyndns.org 홈페이지에서 사용자 이름 및 도메인을 등록한 뒤 공유기를 설정하여야 합니다.

서비스 공급자	ipTIME DDNS
호스트이름	
사용자 계정	
사용자 암호	
• ipTIME DDNS를 사용하실때에는 별도의 등록과정이 필요하지 않습니다. • 호스트이름은 iptime.org 로 끝나야 합니다. (예> testtest.iptime.org) • 사용자계정에는 E-mail주소를 입력해야 합니다. • 한개의 호스트만 등록할 수 있습니다.	
추가	
호스트이름	접속상태
ddnsiptime.iptime.org	등록 시도중
접속상태 다시보기 갱신 삭제	

DDNS 동작을 위하여 설정할 항목은 다음과 같습니다.

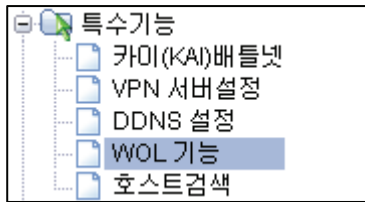
항목	설명
서비스 공급자	ipTIME DDNS 또는 DynDNS 서비스 공급자를 선택합니다.
호스트이름	DDNS 서비스에 사용할 호스트 이름을 설정 합니다.
사용자 계정	DDNS 서비스 이용을 위한 사용자 계정을 입력합니다. ipTIME DDNS를 사용할 경우에는 E-mail 주소를 사용자 계정으로 사용하셔야 합니다.
사용자 암호	DDNS 서비스 이용을 위한 사용자 계정의 암호를 입력합니다.

ipTIME DDNS 암호찾기

ipTIME DDNS 설정시 사용했던 E-mail주소를 입력 후 E-mail보내기 버튼을 클릭합니다.

- ipTIME DDNS 설정 시 사용자 계정으로 입력한 E-mail 주소를 입력한 후 **E-mail 보내기** 버튼을 클릭하시면 해당 메일주소로 암호가 발송 됩니다.

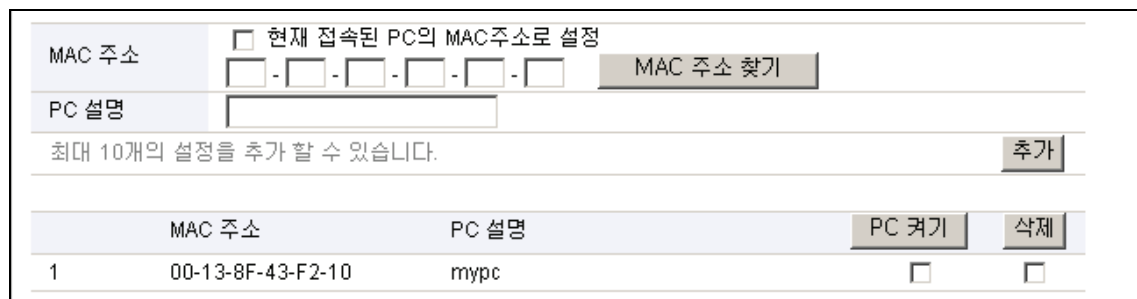
10.4 WOL 기능



WOL(Wake-up On Lan) 기능을 이용하면 공유기에 연결된 PC 전원을 켤 수 있습니다.

즉, WOL을 이용할 경우 인터넷을 통하여 공유기에 접속한 뒤 PC 전원을 켤 수 있기 때문에 사무실이나 가정에 설치된 PC를 외부 어디서든지 사용 하 실 수 있습니다.

- WOL을 이용하기 위해서는 PC에 WOL 기능을 제공하는 LAN 카드가 설치되어야 합니다
- 외부에서 PC를 사용하시기 위해서는 해당 PC에 Windows OS에서 제공하는 원격 데스크톱 기능(XP Professional 이상에서만 지원)을 활성화 하시거나, Remote Admin 또는 VNC 같은 어플리케이션을 이용하시면 됩니다.



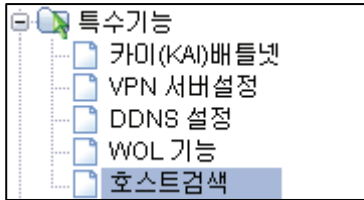
	MAC 주소	PC 설명	PC 켜기	삭제
1	00-13-8F-43-F2-10	mypc	☐	☐

WOL 동작을 위하여 설정할 항목은 다음과 같습니다.

항목	설명
MAC 주소	WOL 기능을 이용할 PC의 MAC 주소를 입력합니다.
PC 설명	해당 PC의 간단한 설명을 입력합니다..

- 등록된 리스트에서 'PC켜기' 항목을 체크하신 후에 **PC켜기** 버튼을 클릭하시면 해당 MAC 주소의 PC의 전원이 켜집니다.

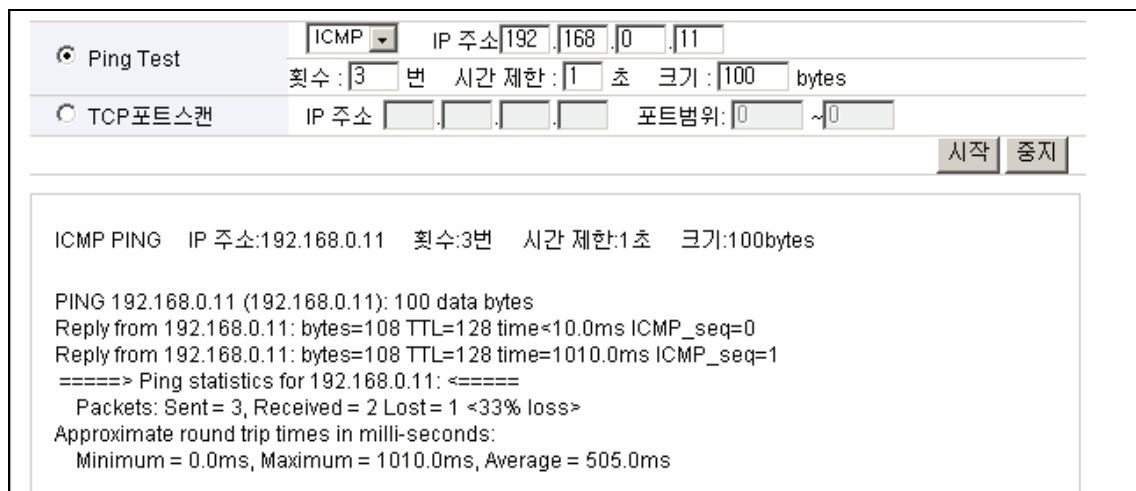
10.5 호스트검색



호스트 검색은 크게 Ping Test와 TCP포트스캔 두 가지 기능으로 나뉘며, Ping Test의 경우 [ICMP]와 [ARP]로 구분됩니다.

Ping Test - ICMP

Ping은 해당 컴퓨터에 소량의 패킷을 보내 되돌아 오는지를 확인하는 것으로 해당 단말(PC)과 지정한 단말(PC)간의 연결 상태를 확인할 수 있습니다.



ICMP Ping Test configuration: ICMP selected, IP 주소: 192.168.0.11, 횟수: 3, 시간 제한: 1 초, 크기: 100 bytes.

Results:

```

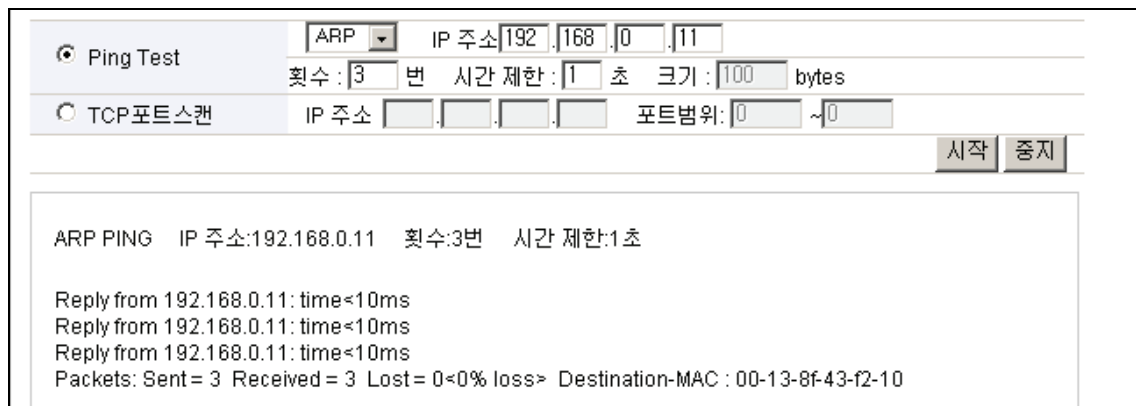
ICMP PING IP 주소:192.168.0.11 횟수:3번 시간 제한:1초 크기:100bytes

PING 192.168.0.11 (192.168.0.11): 100 data bytes
Reply from 192.168.0.11: bytes=108 TTL=128 time<10.0ms ICMP_seq=0
Reply from 192.168.0.11: bytes=108 TTL=128 time=1010.0ms ICMP_seq=1
====> Ping statistics for 192.168.0.11: <====>
    Packets: Sent = 3, Received = 2 Lost = 1 <33% loss>
    Approximate round trip times in milli-seconds:
        Minimum = 0.0ms, Maximum = 1010.0ms, Average = 505.0ms
  
```

- Ping Test항목에서 ICMP 선택하고 Test 대상의 IP주소를 입력한 후에 **시작** 버튼을 클릭하시면 됩니다.

Ping Test - ARP

지정한 IP주소를 가지고있는 PC의 MAC 주소를 알아오는 테스트 방법입니다.



ARP Ping Test configuration: ARP selected, IP 주소: 192.168.0.11, 횟수: 3, 시간 제한: 1 초, 크기: 100 bytes.

Results:

```

ARP PING IP 주소:192.168.0.11 횟수:3번 시간 제한:1초

Reply from 192.168.0.11: time<10ms
Reply from 192.168.0.11: time<10ms
Reply from 192.168.0.11: time<10ms
Packets: Sent = 3 Received = 3 Lost = 0<0% loss> Destination-MAC : 00-13-8f-43-f2-10
  
```

- Ping Test항목에서 ARP 선택하고 Test 대상의 IP주소를 입력한 후에 **시작** 버튼을 클릭하시면 됩니다.

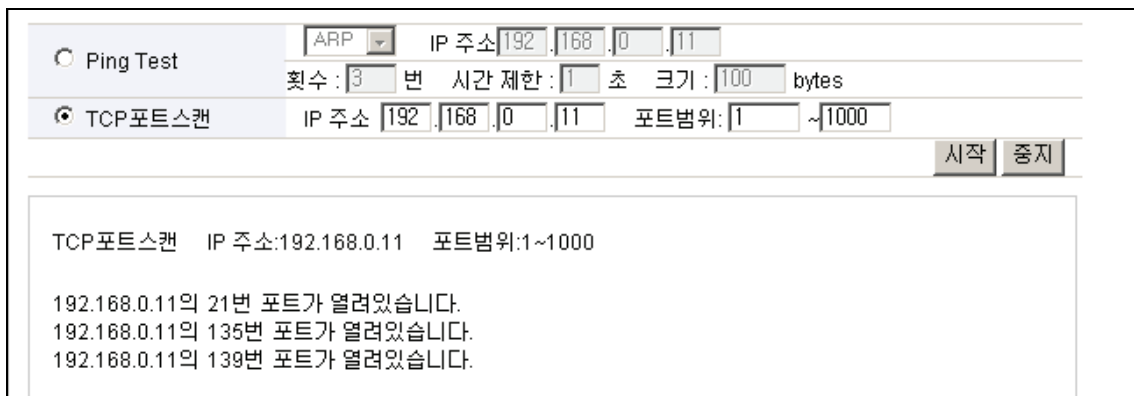
ARP 란?

Address Resolution Protocol의 약자로 상대방의 IP주소를 이용하여 IP주소가 가지고 있는 PC의 MAC 주소를 알아오는 주소 변환 프로토콜입니다.

서로 통신을 하기 위해서는 상대방 랜카드의 MAC 주소를 알고 있어야 하는데, 통신할 송신지(A)에서는 상대방의 MAC 주소를 알지 못하므로, 통신할 수신지(B)의 MAC 주소를 확인하기 위해, 브로드캐스트라는 통신 방법을 사용하여 상대방의 IP주소(B의 IP주소)로 ARP Request를 보내면, 그 IP주소를 가지고 있는 PC(B)가 ARP Response(응답)를 통해 송신지(A)에게 자신의 MAC 주소를 알려주는 과정입니다.

TCP포트스캔

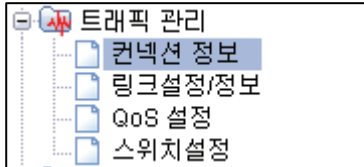
지정한 IP 주소의 PC에서 어떤 TCP 포트가 개방되어 있는지 확인할 수 있는 기능입니다.



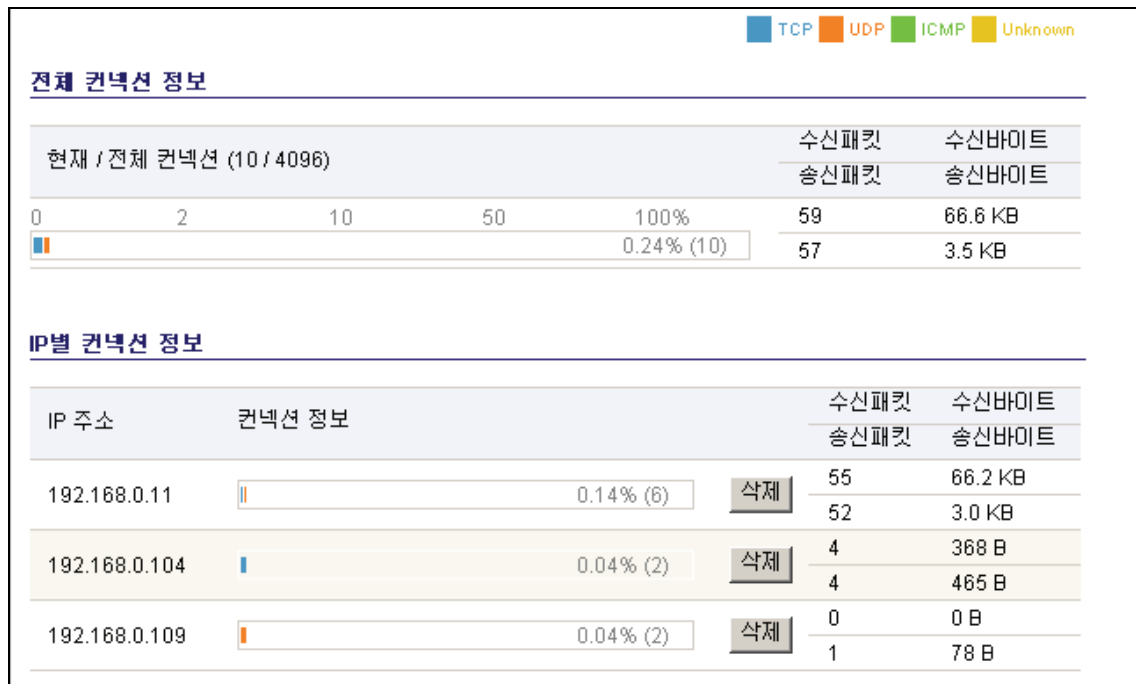
- TCP포트스캔 항목을 선택하고 IP주소를 지정하고 스캔 할 포트의 범위를 입력한 후에 **시작** 버튼을 클릭하시면 됩니다.

11장 트래픽 관리

11.1 컨넥션 정보



ipTIME에 연결되어 인터넷을 사용하는 PC들의 IP주소별로 사용되고 있는 컨넥션의 정보를 보여 줍니다.



전체 컨넥션 정보

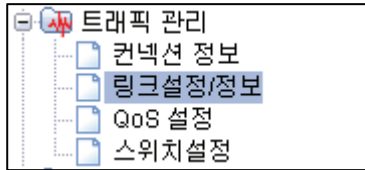
- 현재 통신하고 있는 모든 컨넥션의 개수를 알 수 있습니다.
- 전체 컨넥션의 수는 공유기가 가질 수 있는 최대 컨넥션 수를 나타냅니다.
- 현재 컨넥션 수가 전체 컨넥션 수와 같아지면 더 이상의 인터넷 연결을 할 수 없습니다.

IP 별 컨넥션 정보

- IP 주소란은 연결을 시작한 IP를 나타냅니다.
- 이 정보를 이용하여 과도한 컨넥션을 생성하는 PC를 찾아낼 수 있습니다
- IP 주소별 **삭제** 버튼을 클릭하시면 모든 컨넥션이 삭제됩니다. 만약 해당 IP 주소에서 파일 다운로드와 같은 통신을 하고 있다면 해당 통신은 끊어지게 됩니다.

항목	설명
TCP	대표적으로 HTTP 및 FTP에서 사용하는 프로토콜입니다.
UDP	P2P 검색 및 온라인 게임등에서 많이 사용하는 프로토콜입니다.
ICMP	ping 명령어를 실행하였을 때 사용되는 프로토콜 입니다.
Unknown	3가지 프로토콜 이외의 다른 접속을 의미합니다.

11.2 링크설정/정보



WAN, LAN포트의 동작모드, 속도, Duplex 및 개별 포트의 통신량을 확인할 수 있으며, 특정 포트의 속도를 자동 또는 수동으로 결정 할 수 있습니다.

링크 설정

포트번호	동작모드	속도	Duplex	
WAN	자동	100Mbps	FULL	적용
1	자동	100Mbps	FULL	적용
2	자동	100Mbps	FULL	적용
3	자동	100Mbps	FULL	적용
4	자동으로 고정			

링크 상태 정보

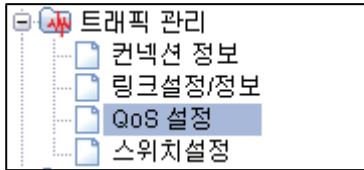
포트번호	WAN	1	2	3	4
Link	On	On	On	Off	Off
속도	100 Mbps	100 Mbps	100 Mbps	-	-
Duplex	Full	Full	Full	-	-

링크 통계 정보

포트번호	WAN	1	2	3	4
Rx-Packets	2363	15103	684	0	0
Rx-Bytes	643273	1306297	80584	0	0
Rx-Broadcast	771	0	0	0	0
Rx-Multicast	0	2306	34	0	0
Rx-Error	0	0	0	0	0
Tx-Packets	1574	14264	1628	0	0
Tx-Bytes	144842	16453443	662294	0	0
Tx-Collision	0	0	0	0	0

- ipTIME 모델마다 LAN포트의 수는 달라질 수 있습니다.

11.3 QoS 설정



QoS를 이용하면 공유기에 연결된 PC의 인터넷 속도를 원하는 대역만큼 제한하거나 보장할 수 있습니다.

QoS를 이용하기 위해서는 먼저 QoS 기본 설정을 통하여 사용되는 인터넷의 대역폭을 정의한 뒤 IP 주소 또는 어플리케이션 포트 번호에 근거하여 인터넷 대역폭을 제한하거나 보장할 수 있습니다.

QoS 기본설정

QoS 기능의 정상적인 동작을 위해서는 공유기가 접속된 인터넷 속도에 대한 기본값을 정확히 설정합니다.

QoS 기본설정			
동작 설정	☒ 실행 ☐ 중단		
인터넷종류	사용자정의		
다운로드	100 Mbps	업로드	100 Mbps
적용			
인터넷속도가 2.5Mbps인 경우에는 2500Kbps로 입력하세요. 소숫점단위로 설정할 수 없습니다. 정확한 인터넷 속도는 speed.nia.or.kr 에서 측정할 수 있습니다.			

QoS 기본 설정을 위하여 설정할 항목은 다음과 같습니다.

항목	설명
동작 설정	실행 또는 중단 을 선택하여 QoS 동작을 설정합니다.
인터넷 종류 다운로드/업로드	해당 서비스의 다운로드와 업로드 속도가 자동으로 입력되며 인터넷 종류를 사용자 정의로 설정하면 다운로드 속도와 업로드 속도를 임의의 값으로 입력할 수 있습니다.

- QoS의 정확한 동작을 위해 <http://speed.nia.or.kr> 등의 속도 측정 사이트에서 정확한 인터넷 속도를 측정한 뒤 사용자 정의로 입력할 것을 권장합니다.
- 인터넷 속도를 수정하게 되면 이미 입력된 IP, 포트, 어플리케이션 별 QoS 설정 규칙이 무의미해지므로 설정된 규칙은 자동 삭제됩니다.

QoS 규칙설정

☒ 사용자 정의 설정
☐ 어플리케이션 설정

IP 주소 ☒ 192.168.0. ~ 192.168.0. ☐ Twin IP

프로토콜 외부포트번호 ~

동작방법 다운로드 Kbps 업로드 Kbps

최대 32개의 규칙이 설정 가능합니다. 적용

☐ 사용자 정의 설정
☒ 어플리케이션 설정

IP 주소 ☒ 192.168.0. ~ 192.168.0. ☐ Twin IP

어플리케이션 WWW(HTTP)

동작방법 다운로드 Kbps 업로드 Kbps

최대 32개의 규칙이 설정 가능합니다. 적용

QoS 규칙 설정을 위하여 설정할 항목은 다음과 같습니다.

항목	설명
IP 주소	규칙이 적용될 IP 주소를 입력합니다. 입력하지 않을 경우에는 모든 IP 주소가 적용 대상이 됩니다.
프로토콜/외부포트번호	규칙이 적용될 프로토콜과 해당 외부 포트번호를 입력합니다.
어플리케이션	규칙이 적용될 이미 정의된 어플리케이션을 선택합니다.
동작방법	최대속도제한: 과도한 인터넷 사용을 방지하기 위해 사용합니다. 최소속도보장: 일정한 수준 이상의 인터넷 속도가 보장되어야 하는 경우 사용합니다
다운로드/업로드	제한 또는 보장을 하기 위한 속도를 입력합니다.

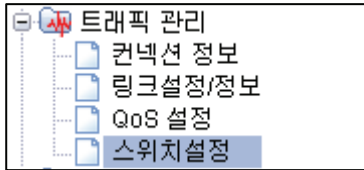
QoS 규칙설정 예제

높은 번호일수록 우선순위가 높습니다.

	IP 주소	프로토콜	동작방법	다운로드	업로드	☐	삭제
1	192.168.0.4		최대 속도 제한	2 Mbps		☐	
2	모든 IP주소	WWW(HTTP)	최대 속도 제한		512 Kbps	☐	
3	192.168.0.100	TCP 8080	최소 속도 보장	3 Mbps		☐	

QoS 설정 예	QoS 동작 방식
192.168.0.4 다운로드 2Mbps 최대 속도 제한	192.168.0.4는 2 Mbps 이상 다운 받을 수 없습니다. 다른 트래픽이 증가하면 다운로드 1Mbps 이하가 될 수도 있습니다. 다른 트래픽이 없는 경우에도 다운로드는 1Mbps로 제한 됩니다
WWW(HTTP) 업로드 512Kbps 최대 속도 제한	512 Kbps 이상의 속도로 업로드할 수 없습니다. 다른 트래픽이 증가하면 업로드는 512 Kbps 이하가 될 수도 있습니다. 다른 트래픽이 없는 경우에도 업로드는 512 Kbps로 제한 됩니다.
TCP 8080 다운로드 3Mbps 최소 속도 보장	3 Mbps 이상의 속도로 다운로드할 수 있습니다. 다른 트래픽이 증가해도 다운로드는 최소 3 Mbps 이상을 유지합니다. 다른 트래픽이 없는 경우 다운로드는 3Mbps 이상이 될 수 있습니다

11.4 스위치설정



스위치 설정에서는 포트미러링, VLAN 및 NAT 하드웨어 엔진기능의 사용여부를 설정할 수 있습니다.

포트미러링

공유기를 통해 통신하는 모든 패킷을 지정된 포트로 복사 전송 합니다.

포트미러링	
☐ 인터넷으로 통신하는 모든 패킷을 1번포트로 전송합니다.	적용

- ipTIME 모델별로 포트미러링 포트가 변경 될 수도 있습니다.

VLAN 설정

VLAN(Virtual LAN)의 기술을 이용하여 물리적 배치와 상관없이 논리적으로 LAN 을 구분할 수 있는 기술입니다.

VLAN의 주된 사용 이유는 트래픽을 줄이고, 여러 워크그룹과 리소스를 분리하고, 허용된 사용자만 접속하도록 제한함과 네트워크의 보안 강화입니다.

VLAN설정					
☐ VLAN간의 Unicast통신을 허용합니다.					적용
최대 5개의 VLAN을 설정할 수 있습니다.					
	삭제	☐ PORT 1	☐ PORT 2	☐ PORT 3	☐ PORT 4 추가
1	☐	PORT 1	PORT 2	PORT 3	PORT 4
2	☐	PORT 1	PORT 2	PORT 3	PORT 4

- 위의 설정 예는 포트 1,2 번과 포트 3,4번을 논리적으로 구분하여 두 개의 VLAN간에는 통신이 되지 않습니다.

NAT하드웨어 엔진기능

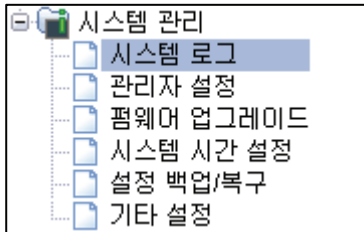
하드웨어 제공하는 NAT 엔진을 사용하여 통신 속도를 향상 시킬 수 있습니다.

NAT하드웨어 엔진기능	
☒ NAT하드웨어 엔진기능 사용	적용

- 일부 장비와의 호환성을 보장하기 위해서 NAT 하드웨어 엔진기능을 끌 필요가 있습니다.

12장 시스템 관리

12.1 시스템 로그



시스템 로그 기능을 이용하면 공유기의 동작 내역을 확인할 수 있으며 저장된 로그를 E-mail 로 전송할 수 있습니다.

최대 갯수 400개가 초과하게 되면 가장 오래된 로그내역부터 삭제되고 최신 로그내역이 추가됩니다.

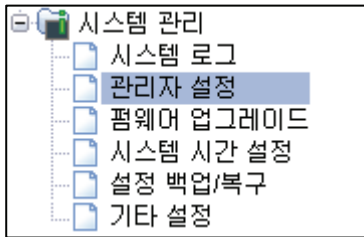
시스템 로그 설정

로그 기능 설정	☒ 동작 ☐ 중지	적용
로그 기능 상태	로그갯수(최대갯수) : 25(400)	전체 삭제
E-mail 보고 기능	[관리자 E-mail을 설정]하여야 E-mail 보고기능을 사용할수 있습니다.	

시스템 로그 보기

발생시간	로그 내용
2007/04/16 21:58:25	모든 설정이 저장됨
*****	PPP가 연결되어 IP를 받음: 211.222.212.208 (WAN1)
*****	PPPoE 서버의 응답이 없음(WAN1 [PAD])
*****	시스템 재시작 (Version : 3.00)

12.2 관리자 설정



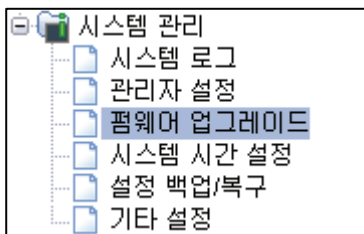
설정 웹 서버 접속 시 사용되는 관리자의 계정 및 암호를 설정 할 수 있고 시스템 로그 및 네트워크 감시 보고서에서 사용할 수 있는 관리자 E-mail 주소를 설정 할 수 있습니다.

로그인 암호 설정	
현재 계정 및 암호	계정 - efrnnet 암호 - 설정됨
새 계정	
새 암호	
새 암호 확인	
적용	

관리자 E-Mail 설정	
관리자 E-Mail	
메일서버(SMTP)	
보내는 E-Mail	
메일 서버 인증	☐ 사용할 ☒ 사용하지 않음
메일 서버 계정	
암호	
적용	

- 공장 출하 시 계정과 암호는 별도로 설정되어 있지 않습니다.
- 로그인 암호를 잊어버린 경우 리셋 스위치를 이용 공장초기화 방법으로 초기화합니다

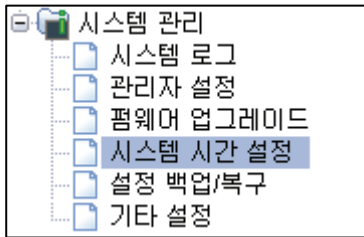
12.3 펌웨어 업그레이드



새로 배포되는 ipTIME 펌웨어를 해당 메뉴에서 업그레이드 할 수 있습니다

자세한 내용은 5장 기본설정의 5.4절 펌웨어 업그레이드를 참고합니다.

12.4 시스템 시간 설정

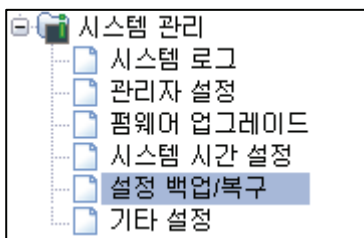


공유기가 인터넷에 연결되었을 때 시스템 시간을 얻어오는 서버와 표준 시간대를 입력합니다. 원하는 Time Server와 시간대를 선택한 후 적용 버튼을 클릭합니다.

현재 시스템 시간	2007년 4월 16일 월요일 21시 59분 47초	
Time Server 설정	time.windows.com time.windows.com	☐ 일광절약시간제 적용
표준시간대	(GMT+09:00) 서울, 도쿄	
적용		

- 인터넷이 연결되어 있지 않거나 Time Server가 동작하지 않는 경우 1970년으로 시간이 표시될 수 있습니다.

12.5 설정 백업/복구

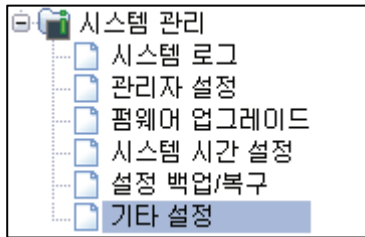


공유기의 설정을 PC로 저장하거나, PC에 저장해둔 설정파일을 공유기에 적용 할 수 있습니다. 또는 공장 초기화 상태로 설정을 복원할 수 도 있습니다.

설정 파일 백업	모든 설정을 설정파일로 저장하며 PC로 다운로드합니다. PC에 저장된 설정파일은 설정 복구시 사용됩니다.
찾아보기...	
설정 파일 복구	PC에 저장해둔 설정파일을 이용해 설정을 복구합니다.
초기 설정 복원	시스템의 모든 설정이 초기화된 후 재시작 됩니다.

항목	설명
설정 파일 백업	모든 설정을 설정파일로 저장하여 PC로 다운로드 합니다.
설정 파일 복구	PC에 저장해둔 설정파일을 이용해 설정을 복구합니다.
초기 설정 복원	시스템의 모든 설정이 초기화된 후 재시작 됩니다.

12.6 기타 설정

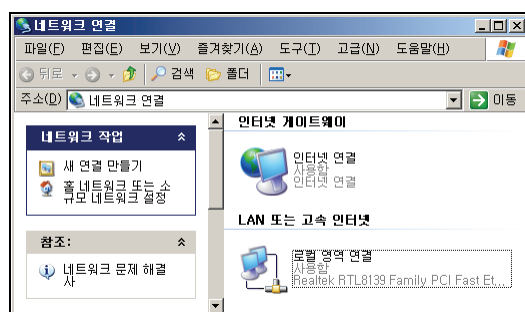


공유기의 이름 설정 및 UPNP 설정 등의 기타 기능들의 동작여부를 설정할 수 있습니다.

공유기 이름		적용
설정화면 자동연결	☐ 실행 ☒ 중단 인터넷 끊김시 공유기 설정화면으로 자동으로 연결되는 기능입니다.	적용
로그인 페이지 설정	☒ 설정 화면 접속시 로그인 페이지를 보여줍니다. ☐ 설정 화면 접속시 로그인 페이지를 보여주지 않습니다.	적용
UPNP 설정	☒ 실행 ☐ 중단	적용
공유기 재시작	공유기가 재시작된 후 "기타 설정" 페이지로 접속됩니다.	적용

항목	설명
공유기 이름	공유기 이름은 웹 설정 화면의 인터넷 탐색기 상단에 표시되는 Title입니다. 원하는 공유기 이름을 입력하고 적용 버튼을 클릭하면 이름이 변경됩니다.
설정화면 자동 연결	설정 화면 자동 연결 기능을 활성화하면 공유기가 인터넷에 연결되지 않은 경우 모든 인터넷 화면을 공유기 설정 화면으로 전환합니다. 이 기능을 이용하면 인터넷이 끊기면 바로 공유기 화면이 접속되어 인터넷 연결 상태를 쉽게 확인할 수 있습니다.
로그인 페이지 설정	공유기의 웹 설정 화면에 접속하는 경우 최초 표시되는 로그인 화면을 보여줄지 여부를 결정합니다.
UPNP 설정	UPnP는 Universal Plug and Play의 약자로 MSN등 MS 윈도우 관련 제품에서 공유기의 존재 여부를 확인하여 여러 가지 서버 프로그램이 정상적으로 수행될 수 있도록 하는 프로토콜입니다.
공유기 재시작	공유기를 재시작 합니다. 만약 저장하지 않은 설정이 있다면 지워지게 됩니다.

- UPnP가 동작하면 XP 윈도우는 아래 그림처럼 인터넷 게이트웨이를 인식하게 됩니다.

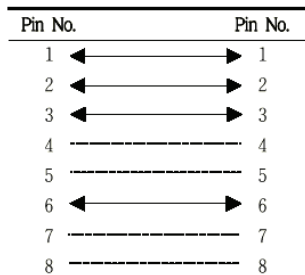
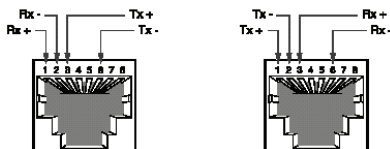


<윈도우 XP에서 UPnP를 통해서 인식된 IP 공유기 아이콘>

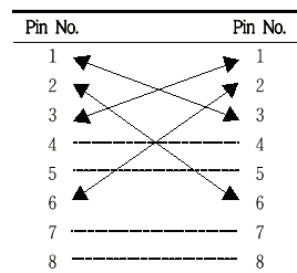
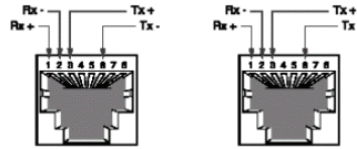
부록 A. LAN Cable 규격

LAN Cable은 스트레이트 케이블(다이렉트 케이블)과 크로스 케이블이 있습니다.

ipTIME에는 케이블 자동 감지 기능이 있어 이 두 가지 케이블 중 어떤 케이블을 사용하여도 됩니다. 그러나 규정에 따라 1-2, 3-6 번 선의 꼬임상이 유지되지 않은 케이블을 사용하면 정상적인 통신이 불가능하므로 꼭 규정에 맞도록 케이블을 제작하시거나 구입하여 사용하시기 바랍니다.



<다이렉트 케이블의 구성>

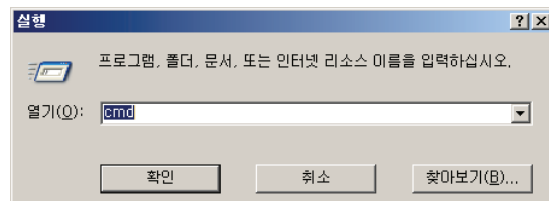


<크로스 케이블의 구성>

부록 B. IP 공유기 Ping 시험

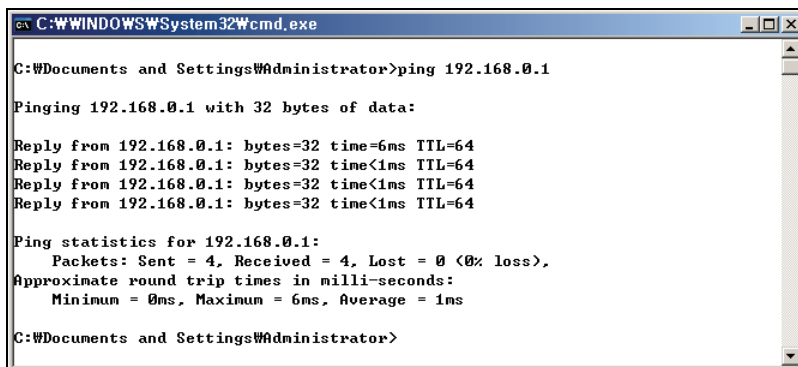
PC가 IP 공유기에 정상 연결되어 있는지 여부는 PC에서 공유기로 Ping 시험을 하면 알 수 있습니다. IP공유기 공유기로 Ping 시험을 하기 전에 PC의 IP 주소가 정상인지를 확인하여야 합니다. PC의 IP 주소 확인은 자동으로 설정한 경우 본 설명서 3장의 내용을 참고하고 수동으로 설정하는 경우 본 설명서 부록 A의 내용을 참고합니다.

- Ping 시험을 하기 위해서는 Win98/ME의 경우 MS-DOS를, Windows 2000/XP의 경우 명령 프롬프트를 실행합니다. 이의 실행을 위하여 윈도우 화면 좌측 하단의 "시작" 버튼을 클릭하고 "실행"을 선택합니다.
- 열기 윈도우에서 98/ME의 경우 "command"를 2000/XP의 경우 "cmd"를 입력하고 확인 버튼을 클릭하여 MS-DOS 또는 명령프롬프트를 실행합니다.



<command 또는 cmd 실행>

- MS-DOS 또는 명령프롬프트 윈도우에서 "ping 192.168.0.1" 명령을 입력합니다.



<Ping 192.168.0.1 명령 실행과 그 결과>

위의 그림과 같이 "Reply from...." 4개 메시지가 확인되면 IP 공유기와 PC가 정상적으로 연결되어 있어 통신에 문제가 없는 것을 확인할 수 있습니다.

